VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATION TECHNOLOGIES

STRATEGIE FIRMY PRO ELEKTRONICKÝ OBCHOD – PLATEBNÍ KARTY

COMPANY POLICY FOR ELECTRONICAL BUSINESS – CREDIT CARDS

DISERTAČNÍ PRÁCE

DISSERTATION THESSIS

AUTOR PRÁCE **ING. VLADIMÍR ŠULC**

AUTHOR

ŠKOLITEL **PROF. ING. JIŘÍ DVOŘÁK, DrSc.**

SUPERVISOR

BRNO 2008

RESUMÉ

Předložená disertační práce se zabývá problematikou firmy v elektronickém obchodování, která představuje krátkodobé nebo dlouhodobé záměry v oblasti řízení finančních vztahů k vnějšímu okolí, ale i rovněž uvnitř podniku. Je zde rozebrána problematika možného zneužívání platebních karet. Podnětem pro výběr tématu bylo stále častěji se vyskytující padělání a zneužívání platebních karet. Při podrobnějším zkoumání dané problematiky se zákonitě narazí na problém související s nedostatkem informací o tomto druhu specifické kriminality. Rovněž tak klienti jednotlivých peněžních ústavů často nemají základní informace o možnostech zneužití jejich karet. Proto vyvstává v úvahu i otázka jisté, alespoň minimální základní osvěty ze strany ústavů, jež mají chránit finanční prostředky svých klientů.

Připravovaná disertační práce si klade za cíl vytvoření metodiky zkoumání padělání platebních karet, a to nejenom v rámci České republiky, ale i ve stále se rozšiřujícím systému zemí Schengenské dohody a Evropské unie. Přínos disertační práce lze spatřovat v rovině teoretické i praktické.

V teoretické části disertační práce je provedena analýza současného stavu vědeckého poznání v oblasti informační a komunikační technologie firem, která je implementována do informačních systémů. Dále jsou zde posouzeny výhody a nevýhody, které jsou s touto formou elektronického obchodu spojeny. Jsou zde rovněž charakterizovány specifické možnosti zneužívání platebních prostředků. Tuto problematiku vidím především ve zpracování odborné publikace, jež se bude komplexně zabývat problematikou zneužívání a padělání platebních karet a její možné využití při výuce na policejní akademii. Její stěžejní částí bude charakteristika jednotlivých forem padělání karet a rovněž možná identifikace těchto padělků. Tato publikace by také mohla posloužit i k prevenci a informovat tak klienty peněžních ústavů o možnostech zneužívání platebních karet.

V praktické části práce, která je zaměřena na český a zahraniční trh, jsou určeny základní předpoklady pro realizaci a bezpečné obchodování firem a její postup. Dále je provedena analýza příčin zneužití elektronického obchodování v České republice a jsou zde představeny též výsledky kvantitativního výzkumu, který byl zaměřen na zjištění příčin nízkého zájmu informací mezi veřejností. V závěru je shrnuta zkoumaná problematika a jsou zde nastíněny perspektivy a možnosti dalšího vývoje. Doufám, ze výsledky práce se mi podaří v rámci navrhované disertační práce naplnit a že tato práce nalezne uplatnění i v různých podobách jako jsou (učební texty, případové studie aj.) v pedagogickém procesu.

ABSTRACT

This dissertation work deals with the subject of a company in the area of e-commerce, which represents short-term or long-term plans in controlling the financial relationship toward the outer environment but also inside the company. The problem of possible abuse of credit cards is briefly analysed as well. The impulse for choosing this topic was increasing number of falsification and abusing of credit cards. When this subject is analysed in detail, the problem connected with lack of information on this particular area of crime inevitably appears. Clients of individual banking institutions often do not have even the basic knowledge about the ways their cards could be abused or misused. This is why the question of certain, at least minimal, basic information campaign done by the banks, which are supposed to protect the financial means of their clients.

This dissertation work sets its goal in creating the methods of investigation of credit cards abuse not only in the Czech Republic but in the growing system of countries of Schengen Treaty and European Union. The benefit of the work can be seen in the level of theory as well of practice.

The theoretical part of the work contains the analysis of the current situation of scientific knowledge in the area of information and communication technology of companies, which is implemented into information systems. Then the advantages and disadvantages connected with this kind of e-commerce are assessed and the specific opportunities for abuse of these media of payment are characterised. The problem sees mainly in writing a specialised publication, which would deal with the problem of abuse and falsification of credit cards and its possible use would be at police academies. Its main part should be the characteristics of particular forms of cards forging and also possible identification of these forgeries. This book could also help in prevention and inform clients of financial institutions about the ways of credit cards abuse.

In the practical part, which concentrates on the Czech and foreign market, the author sets the basic premises for realisation of safe business of companies in the Czech Republic and its procedures. Furthermore the reasons of e-commerce abuse in the Czech Republic are analysed and results of quantification research presented. This was concentrated on ascertainment of reason of low interest in information among the public.

In the conclusive part of the work the whole problem is summarised and there are also outlined perspectives and possibilities of further development

The author plans to exploit the results of his work in his dissertation and it will find its use in various ways, such as teaching materials, case studies, etc. In the process of pedagogical work.

BIBLIOGRAFICKÁ CITACE DISERTAČNÍ PRÁCE

ŠULC, V. *Strategie firmy pro elektronický obchod – platební karty*, disertační práce, vydáno v Brně, VUT v Brně, Fakulta podnikatelská, rok vydání 2008, počet stran 117, vedoucí disertační práce Prof. Ing. Jiří Dvořák DrSc.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem disertační práci zpracoval samostatně na základě studia uvedené literatury a pod vedením svého školitele.

V Brně dne 30. prosince 2008 .....

Vladimír Šulc

PODĚKOVÁNÍ

Rád bych touto cestou poděkoval svému školiteli, Prof. Ing. Jiřímu Dvořákovi, DrSc. za cenné metodické a odborné rady, které mi poskytl jak v průběhu doktorandského studia, tak při zpracování disertační práce.

Mé poděkování patří rovněž Ing. Jiřímu Křížovi, PhD., řediteli Ústavu informatiky Fakulty podnikatelské VUT v Brně, při zpracování této práce.

Na tomto místě bych chtěl poděkovat rovněž svým nejbližším, zejména rodině za stálou a hlubokou podporu v průběhu zpracování disertační práce i během celého doktorandského studia.

Na závěr bych si dovolil vyjádřit své poděkování všem bankovním institucím, které se podílely na primárním výzkumu této práce.

KLÍČOVÁ SLOVA

Bezkontaktní platby, bílí koni, hacker, lobisti, magnetický proužek, MasterCard, mikročip, skimmmování, terminál, úvěruschopnost , vertifikační číslo

.

KEY WORDS

Contactless payments, white horse, hacker, lobbyists, magnetic strip, MasterCard, microchip, skimming , terminal , creditworthiness, verification number

OBSAH

1 ÚVOD

Elektronické obchodování jde mílovými kroky dopředu, o tom nikdo z nás asi nepochybuje. Informační systémy a informační technologie se staly během krátké doby strategickým faktorem úspěšnosti a [1]konkurenceschopnosti podniku. Potřeba kvalitního informačního systému je vynucena především charakterem současného hospodářského prostředí, v němž stale významnější úlohu hrají informace. Ještě před dvaceti lety málokdo věděl, co je to platební karta. Myšlenka, že byste se vydali do obchodu bez peněz a přesto si mohli něco odnést, nepřicházela v úvahu. Chodit na nákupy bez hotovosti není v současnosti téměř žádný problém, naopak se tato móda stává nedílnou součástí našich každodenních životů. U některých z nás je běžné, že nákupy provádíme přes internet a platba je prováděna přímo z účtu klienta.

Historicky nejstarší písemné záznamy o použití platebního prostředku pocházejí z doby staré cca 4500 let a dochovaly se v oblasti starověké Mezopotámie, což je území dnešního Iráku.

Je známo, že lidé jako platidel používali nejprve různé materiály. Následně bylo používáno vážené množství stříbra a pak již byl krok k vyhotovení mincí. První byly vyraženy r. 640 až 630 př.n.l. v Lýdii, avšak už Číňané v 11. století tiskli papírové stvrzenky v pevných hodnotách a používali je jako peníze. Na území dnešní České republiky byly papírové peníze v tehdejším Rakousku – Uhersku zavedeny dekretem císařovny Marie Terezie v roce 1762. Vydáním papírových zlatek konvenční měny zvaných „bankocedule“ byla zmocněna Vídeňská městská banka.

V dějinách se vždy našli lidé, kteří se snažili výrobou falešných mincí a bankovek obohatit sami sebe, či dokonce ohrozit finanční hospodářství a ekonomiku celého státu. Souběžně s výrobou a užíváním platebních prostředků se začalo rozvíjet i padělatelství. Přitom se toto považovalo za těžký zločin a trestalo se v různých státech např. deportací, usekáváním rukou, hozením zaživa do vroucí vody či oleje nebo popravou. U nás se v této době trestalo padělatelství zabavením majetku, upalováním, škrcením nebo smýkáním. Pro zajímavost lze uvést, že již za Rakouska – Uherska byl tehdejší národní bankou zaveden systém řazení padělků do typů a uvádění stupně jejich nebezpečnosti. Tento systém převzala a používá dodnes Česká národní banka.

[1]GRUBLOVÁ, E. - PRUSÁK, J, - PŘADKA, - M, STEINOVÁ, M. *Internetová ekonomika*. Ostrava.2002.ISBN 80 – 7329-000-6

Na koncipování finanční strategie firmy mají klíčový význam zejména prostředí, ve kterém podnik působí, zákazníci, stát i věřitelé a situaci samotného podniku jako je konkurenceschopnost, systém řízení, finanční situace apod.

Problematiku elektronického obchodování jsem si za téma své disertační práce vybral proto, že v podmínkách českého kapitálového trhu není zatím dostatečná informovanost o této problematice. Jedním ze základních pilířů elektronického obchodování jsou platby prováděné pomocí platebních karet.

V novodobé historii českého trhu se dosud uskutečnilo několik prvotních informací, upozorňujících na způsoby zneužívání platebních karet, počínaje způsoby primitivními až po velmi kvalifikované zásahy do elektronických údajů zakódovaných v elektronickém médiu (magnetických proužcích nebo mikročipech) platebních karet. Na základě výše uvedeného se domnívám, že zvolené téma disertační práce je v současné době aktuální .

2 CÍLE DISERTAČNÍ PRÁCE

2.1 SYSTÉMOVÉ VYMEZENÍ PROBLÉMU

Integrace obchodních aktivit firem je součástí globalizace v elektronickém prostředí. Tento proces zahrnuje integrační tendence jak v horizontálním i vertikálním směru. Přesouvá se oblast klasického strategického řízení na zákaznickou platformu individuálního zakázkového řízení s uplatněním kybernetických principů v elektronickém prostředí obchodování. Vzrůstá potřeba informační gramotnosti s novými aspekty znalostní gramotnosti. V modelech se uplatňují nové principy hierarchického řízení s akcentem technického vyjádření prostředí – informačními a komunikačními technologiemi.

Systémové pojetí práce je základním pohledem na ucelený proces B2C s vymezením mezních stavů a získání tak bezpečného prostředí elektronického obchodování. V této práci je vybrána modelová představa integrovaného elektronického obchodování a jeho strategie s akcentem velmi zajímavé oblasti bezhotovostních plateb realizovaných platebními kartami v prostředí rizik zejména technického a technologického prostředí. Model bezpečného využívání platebních karet tvoří nedílnou součást moderního pojetí strategie elektronického obchodu firem a bude tvořit znalostní pohled na rozvíjené oblasti e-ekonomiky a v EU nového pojetí prostředí e-Europe.

Průřezová oblast této práce je spjata se systémovým řešením řízení a ekonomiky podniku a kybernetickým vyjádřením řetězce obchodních aktivit v této oblasti s akcentem na bezpečné provozování finančních aktivit pomocí platebních karet. Hlavní pozornost se nyní věnuje bezpečnému obchodování a tedy i bezpečnému využívání platebních karet a rizikům souvisejících s technickými prostředky těchto instrumentů.

2.2 VYMEZENÍ CÍLŮ PRÁCE

V teoretické části práce bude, v souladu s názvem práce, provedena především systémová analýza elektronického obchodování firem v oblasti informačních a komunikačních technologií, moderní strategie elektronického obchodu firem a funkce bezhotovostního styku v moderních koncepcích strategie elektronického obchodování firem. Stěžejním cílem bude analýza bezpečných plateb a rozbor modelu finančních transakcí platebními kartami zejména v agresivním uživatelském prostředí.

Hlavním cílem praktické části této práce je vymezení modelu elektronického obchodu a základních předpokladů pro bezpečné platby s důrazem na přímé platby realizované

platebními kartami v uživatelském prostředí s vymezenými mezními stavy tohoto ekonomického kyberprostoru v řízení podniků.

Dílčí cíle budou především zaměřeny na:

- provedení hlubší analýzy problematiky bezhotovostních plateb, zejména s použitím platebních karet, které představují globálně rozšířený moderní platební prostředek. Hlavní pozornost přitom soustřeďuji především na způsoby a prostředky, které eliminují možnosti jejich zneužití na přijatelné riziko,
- základě hlubšího poznání řešené problematiky vytvořit návrh nových řešení a postupů, jejichž realizací bude možno dosáhnout podstatně vyššího stupně elektronického obchodování i ochrany bezhotovostních plateb a tedy i využívání platebních karet s ochranou před jejich zneužitím.

3 METODY ZPRACOVÁNÍ DISERTAČNÍ PRÁCE

Při volbě metod, budou použity při zpracování disertační práce, je nutné vycházet z následujícího požadavku: „použít takovou množinu metod, povede disertační práci k naplnění jejich základních cílů a bude metodologicky akceptovatelná a efektivní“. Při zpracování disertační práce budou využity zejména metody založené na myšlenkovém postupu, tzv. metody logické, které patří do skupiny metod systematického způsobu tvořivého myšlení, ale také zkušenosti získané v ostatních oborech.[2]

Podstatou této rozhodující skupiny metod tvořivosti je tzv. systematické myšlení. Vychází ze současného stavu vědeckého poznání jevů a procesů a z logiky zákonitosti vývoje analyzovaných problémů. Společným metodickým základem systematického způsobu tvořivosti jsou vědecké metody poznání. Využívají se hlavně tyto:

- metody logické
- metody empirické
- metody založené na modelování a analogii

3.1 METODY LOGICKÉ

Logické metody jsou tvořeny souborem postupů, které k dosažení stanoveného cíle využívají principy logiky a logické myšlení řešitele. Patří k nim tato trojice „párových metod“:

„indukce –dedukce“ , analýza – syntéza“ , „abstrakce – konkretizace“

Indukce je proces posuzování jedinečných výroků či jedinečných poznatků o charakteristikách prvků u jednotlivých objektů, který vede k obecnému poznání. Indukce je úsudek směřující od zvláštních případů k obecné poučce. Metoda indukce řeší vztah mezi porovnanými údaji a teorií tak, že na základě shromážděných empirických poznatků se vyvozují obecné závěry o stavu vývoje dané reality.[3] **Dedukce** je proces vyvozování konkrétnějších, inviduálních poznatků z poznatků obecnějších (tzv. premis) Jinými slovy, je to proces, u něhož se z premis, s použitím určených pravidel logiky, dospívá k novému tvrzení a vyvozuje se určitá souvislost nutná pro konkrétní případ. Je to proces přechodu od obecného ke specifickému, tedy opak indukce.

[2] MERVART, J. *Základy metodologie vědy*. 1. vyd. Praha: Svoboda,1977.186s. ISBN 25-067-77

[3] JANÍČEK, P. – ONDRÁČEK, E. *Řešení problému modelování*. 1. vyd. Brno: 1998.ISBN 80-124

Analýza je vědecká metoda založená na dekompozici celku na elementární části. Jde o myšlenkové rozčlenění objektu na části, vymezení jeho určitých znaků a jejich samostatné zkoumání a poznání jejich podstaty a zákonitostí.[4]

Syntéza – jde o myšlenkové spojení předmětů nebo jevů v celek, tvořící obraz reálné skutečnosti (montáž), má však jako metodologický princip analýzu vždy doplňovat.[5]

Abstrakce a zobecnění – jde o myšlenkové vymezení, vybrání jednotlivých, v dané úvaze podstatných znaků jevu nebo předmětu a ponechání všech ostatních znaků bez prozkoumání.

Často se pojmu abstrakce užívá i v tom smyslu, že v rámci myšlení vylučujeme při řešení problému vše nepodstatné. Tím se umožní dostat se k podstatě problému
(např. abstraktní model řešení).

3.2 METODY EMPIRICKÉ

Okruhy metod a technik kvalitativního a kvantitativního výzkumu není možné přesně rozlišit, protože mnohé se, po případné lehké modifikaci, využívají jak v jednom, tak i druhém výzkumu. K základním metodám empirického výzkumu se obvykle řadí dotazování (nejběžnější a nejčastěji využívaná metoda založená na výpovědích respondentů), pozorování (zachycuje zejména chování lidí v nejrůznějších situacích, reakce lidí na měnící se podněty, interakce člověka s druhými lidmi i s předmětným prostředím), experiment (výzkumník mnoha různými způsoby vstupuje aktivně do zkoumaných skutečností) a analýza věcných skutečností (zahrnuje jak skutečnosti, které vzniky spontánně, tak ty, které byly zadány jako úkol).

3.3 METODY ZALOŽENÉ NA MODELOVÁNÍ A ANALOGII

Metoda modelování spočívá ve zkoumání reálných objektů pomocí jiných, zpravidla uměle konstruovaných objektů, v nichž jsou vyjádřeny, charakterizovány a definovány pouze vybrané vlastnosti, stránky a vztahy originálního objektu. Vychází ze stanoviska, že model je mezičlánek mezi realitou a teorií o realitě a má důležitou funkci v procesu poznání. Způsoby (techniky) modelování se mohou značně lišit, a to podle toho, jaké

[4] GEIST, B. *Sociologický slovník*. 1 . vyd. Praha: Victoria Publishing, 1992. ISBN 80-85605-28-7

[5] JANÍČEK, P. – ONDRÁČEK, E. *Řešení problému modelování*. 1. vyd. Brno: 1998.ISBN 80-124-1233-X

užívají charakteristiky verbální, grafické, schematické, symbolové, matematické, ekonometrické i jiné.[6] Některé z modelů nevyjadřují nic jiného než jednoduché schéma, které zachycuje jen některé vztahy systému nebo pouhý slovní popis těchto vztahů. Okruhy metod a technik kvalitativního a kvantitativního výzkumu není možné přesně rozlišit, protože mnohé se, po případné lehké modifikaci, využívají jak v jednom, tak i druhém výzkumu.

Každý proces modelování a simulace ekonomického prostředí má vyhodnocení a zpětnou transformaci modelu do reálného prostředí života ekonomického systému. Celý proces identifikace a modelování, resp. simulace a vyhodnocování, musí být proveden v reálném čase (tj. čas, kdy fyzikální veličiny ovlivňující ekonomické prostředí jsou využitelné - mají svoji regulační nebo řídící hodnotu). Proto se v současné době k modelování (resp. simulacím) používají výkonné počítačové systémy. Rovněž tak identifikace prostředí je již moderně prováděna - zatím experimentálně, přímo, a to rozpoznáváním ekonomického prostředí pomocí inteligentních technických čidel.

Obecně se tvorbou modelů zabývá teorie identifikace, v níž lze použít metody známé z teorie umělé inteligence, tj. například rozpoznávání prostředí a scény.

Tvorba modelu ekonomického systému je vždy (stejně jako u obecných systémů) vázána **jazykem jako prostředkem pro sdělování informací** mezi systémy. Jazykem může být jazyk **mateřský** – potom vytvořený model je modelem verbálním, nebo také jenom verbálním popisem zkoumaného systému. Tato forma modelu získává vlastnosti mateřského jazyka – to znamená, že je poznamenána syntaxí a sémantikou jazyka a jeho nejednoznačností (množstvím homonym a synonym jazyka).

5 MERVART, J. *Základy metodologie vědy*. 1. vyd. Praha: Svoboda,1977.186s. ISBN 25-067-77

4 PŘEHLED SOUČASNÉHO STAVU VĚDECKÉHO POZNÁNÍ

4.1 TEORETICKÉ VYMEZENÍ ELEKTRONICKÉHO OBCHODU

Elektronický obchod zahrnuje jakoukoli obchodní operaci, nejčastěji nákup věcí, která je realizována na dálku, prostřednictvím počítačů, počítačové sítě a speciálního programu, jehož prostřednictvím prodávající jednak generuje neurčitému okruhu zájemců svoji nabídku, jednak uzavírá smlouvy. Je to obchod realizovaný na základě smluv na dálku, tedy slovy zákona, smluv uzavřených za použití prostředků komunikace na dálku, které umožňují uzavřít smlouvu bez současné fyzické přítomnosti smluvních stran.

Elektronickým platebním prostředkem je:

a) prostředek vzdáleného přístupu k peněžní hodnotě, při jehož užívání se zpravidla vyžaduje identifikace držitele
b) elektronický peněžní prostředek
c) elektronický peněžní prostředek je platební prostředek, který uchovává peněžní hodnotu v elektronické podobě a který je přijímán jako platební prostředek i jinými osobami než jeho vydavatelem
d) elektronickými penězi je peněžní hodnota uchovávána na elektronickém peněžním prostředku

Elektronický obchod rozdělujeme na dvě kategorie:

1) Elektronické obchodování (e-business) – Podpora provádění obchodní transakce prostředky informačních technologií (typicky i Internetem) a příslušnými aplikačními programy.
2) Elektronické podnikání (e-commerce) – Podpora (některých) oblasti v podnikání prostředky ITS se jedná o oblast řízení vztahů se zákazníky (tzv. CRM) a příslušnými aplikačními programy, řízení dodavatelských řetězců (tzv. SCM)

Elektronické obchodování je součástí informační společnosti a je to forma [7]obchodních operací, při které spolu partneři komunikují mnohem více elektronickou cestou než

[7] DVOŘÁK, J.- KŘÍŽ, J.- DVOŘÁK, J. *Elektronický obchod.* Skripta VUT v Brně, Fakulta podnikatelská 2005

fyzicky (např. při osobních setkáních, apod.). Znamená to, že převažují aktivity jako výběr zboží v ***kybrerprostoru,*** dohodnutí obchodních podmínek e-mailem, elektronická objednávka, převod peněz elektronickou cestou, atd.

Je to způsob podnikání využívající informačních a komunikačních technologií, jak v oblasti řízení podniku, tak v oblasti spolupráce s partnerskými podniky, v oblasti nákupu a prodeje, poskytování služeb zákazníkům atd.

4.2 ZÁKLADY ZÁMĚRU ZAVÉST V PODNIKU ELEKTRONICKÝ OBCHOD

Základy pro úspěšné naplnění záměru zavést v podniku elektronický obchod je:

- kvalitní, průchodná, spolehlivá ***infrastruktura*** lokální podnikové sítě zaručující bezpečné datové přenosy,
- propojení páteřního segmentu lokální ***sítě*** do Internetu vysokorychlostním spojem,
- servery určené k poskytování ***klientských služeb*** vybavené robustním hardwarem s vyhovujícími technickými parametry a vhodným operačním systémem, který garantuje bezpečnost dat uložených v tomto systému,
- aplikační programové ***vybavení,*** splňující veškeré funkční a bezpečnostní požadavky a poskytující srozumitelné a pohodlné uživatelské rozhraní,
- kvalifikovaný a vyškolený ***personál***, zajišťující funkčnost všech výše jmenovaných složek.

Pro rozvoj elektronického obchodu firem je nezbytná strategie elektronického obchodu. ***Strategie*** vyjadřuje základní představy o tom, jakými způsoby budou vytyčené ***strategické cíle*** naplněny. Je to množina dlouhodobých cílů a cest jejich realizace.

4.3 STRATEGICKÝ CÍL

Rozhodování o strategických cílech je ovlivňováno:

- ***prostředím*** v němž firma působí (volba tohoto prostředí bude nyní ovlivňována postupujícími záměry konkurentů v rozvíjejícím se elektronickém obchodování, efektivním využívání informačních a komunikačních technologií v řadě oblastí daného okolí firmy apod.),
- očekáváním důležitých ***„stakeholders“*** působících v okolí firmy,

- objemem dostupných ***výrobních faktorů*** (obsáhnutím informačních zdrojů a jejich spojením),
- interními ***vztahy*** (vztahem vnitřní struktury firmy k informační společnosti),
- ***schopnostmi*** manažerů (informační gramotností a předpoklady pracovat s novými informačními komunikačními prostředky - technologiemi),
- ***znalostí dynamiky*** vývoje firmy (extrapolace vývojových trendů a predikce datového obsáhnutí této strategie firmy).

Strategické cíle musí být vždy spojovány s dynamikou celého systému strategického řízení a jeho bezprostředního okolí. Změna strategie je spojena s analýzou strategické mezery a ta může být spojována s novými kvalitativními změnami v informačních a komunikačních technologiích, jejich provozování resp. v jejich inovacích.

Významné místo v rozvoji elektronického obchodu firem mohou sehrávat stávající ***strategické obchodní jednotky*** vymezené svým organizačním uspořádáním a strategicko-marketingovým posláním.

Hierarchie firemních strategií corporate, business a functional zatím musí integrovaným způsobem propojovat odpovídající úrovně informačního systému elektronického obchodu.

V hierarchii strategií patří informační strategie zatím mezi funkční. Měla by v návaznosti na nadřazené strategie, vyjádřené v obchodní strategii SBU, vymezovat korespondující strategické cíle elektronického obchodu.

Strategie elektronického obchodu musí nově podporovat jak nadřazenou obchodní strategii, tak i všechny ostatní funkční strategie tak, aby integrujícím směrem naplňovala dílčí strategické cíle souvisejících funkčních strategií.

4.4 KONCEPCE INFORMAČNÍHO ZABEZPEČENÍ ELEKTRONICKÉHO OBCHODU

Musí vycházet z analýz identifikujících stávající strategie a vymezující příslušná SBU. Rámcově musíme vycházet z těchto kroků:

- ***analýza a výběr trhu*** - důkladně analyzovat cílový trh. Po vlně tzv. krachů elektronických obchodů ve světě dodnes převládá mylný názor, že elektronický obchod nemá budoucnost,…
- ***budování elektronického obchodu*** - nabízí se nám několik možností, jak toho dosáhnout:

- vlastní výstavba nebo zakázka,
- obchod v „krabici“,
- pronájem aplikace - ASP (Application Service Providing), …

- ***struktura elektronického obchodu firmy*** – v budoucnu bude převládat ***zakázkový systém*** u řady výrobků.

Internet je zatím považován za ***nejlevnější „obchodní prostor***“. Za největší přínosy Internetu je [8]považována možnost oslovení většího obchodního prostoru, snížení cen a doby nutné k uvedení produktu na trh, možnosti dosažení lepší úrovně servisu a komunikace se zákazníkem a zejména přímé ovlivňování zakázkové výroby koncovým uživatelem právě přes informační a komunikační technologie elektronického obchodu.

4.5 INFORMAČNÍ SPOLEČNOST

Je chápána jako soubor nástrojů výpočetní a komunikační techniky a komunikačních a informačních služeb, které se stávají postupně určujícím faktorem rozvoje ekonomiky a významně ovlivňují rozvoj celé společnosti. Jde o celkové prostředí, ve kterém se odehrává život lidí, než o pouhý soubor prostředků informatiky. Představuje celkovou filosofii práce s informacemi, spočívající v tom, že informace nejsou chápány samoúčelně. Člověk je neshromažďuje jen proto, aby je měl, ale proto, aby se podle nich rozhodoval ve zcela konkrétních životních situacích. Cesta k informační společnosti je podporována současnou technologickou revolucí, která je založena na vzájemném propojení např. informačních, komunikačních a mediálních technologií.

Nejvýznamnějším rysem informační společnosti je posun od uzavřených interních informačních systémů k otevřeným systémům využívajícím externí komunikace. ***Internet*** umožňuje masové propojení informačních zdrojů a prostředků, zpracování informací prakticky na celém světě, a stává se tak důležitým nástrojem pro rozšíření nových služeb. Splývání informačních, komunikačních a mediálních technologií podpoří v následujících letech rozvoj klíčových průmyslových odvětví. Informační společnost na jedné straně přinese nové možnosti pro rozvoj ekonomiky a uplatnění vysoce kvalifikovaných pracovníků.

[8]DVOŘÁK, J.- KŘÍŽ, J.- DVOŘÁK, J. *Elektronický obchod.* Skripta VUT v Brně, Fakulta podnikatelská 2005

Ve vztahu k elektronickému obchodování plní Internet následující funkce:

- síť pro ***globální*** (tj. celosvětovou) komunikaci uživatelů
- prostředí zajišťující řadu různých ***komunikačních služeb***
- prostředek pro ***přístup k informacím***
- prostředí pro ***vytváření různých (tj. včetně obchodních) aplikací*** (prodej, marketing,…)
- prostředí pro vytvoření ***globálního elektronického tržiště***

Internet má následující základní rozdíly:

- ***interaktivnost*** (tj. možnost okamžité zpětné vazby od zákazníka)
- možnost ***personalizace/customizace*** (tj. přizpůsobení informacím či produktu dle požadavků daného zákazníka)
- ***distribuční kanál***

4.5.1 Přínosy informační společnosti:

- pro podnikání - vznik nových cest a příležitostí pro podnikání, jako jsou např. marketing, ***elektronický obchod***, „neskladové“ zásobování, elektronické publikování, šíření videoprogramu na vyžádání (video-on-demand), práce na dálku (teleworking) a práci ve virtuálních týmech, elektronické vzdělávání,….
- pro občany - vznik nových možností pro občany - využití jejich kvalifikace a širší možnosti jejich uplatnění, zlepšení a zjednodušení komunikace,…
- pro celou společnost vyšší kvalitu života

4.6 VLIV NA HOSPODÁŘSKÉ PROSTŘEDÍ

Elektronický obchod značně ovlivňuje celé ***hospodářské prostředí***:

- zvyšuje se konkurence z důvodu možnosti každého ekonomického subjektu pronikat na jakýkoliv trh
- dochází k splývání doposud oddělených odvětví (energetika, obchod, výpočetní technika atd.)
- mění se forma komunikace mezi firmami a partnery
- mění se styl prodej výrobků, služeb a také informací
- vznikají elektronické peníze a zvyšuje se podíl bezhotovostních plateb
- dochází k uzavírání nových obchodních dohod na základě využívání společných datových zdrojů

- mění se styl práce, dochází ke vzniku virtuálních týmů a firem, občané mohou komunikovat se stáními institucemi mnohem efektivněji, lze velice snadno realizovat různé průzkumy atd.

Klíčovým aspektem provozování elektronického obchodu je jeho ***bezpečnost***, která úzce souvisí s identifikací a autentizací obou stran e-obchodu, bezpečností plateb, dokazováním a auditováním uskutečněných transakcí, ochranou osobních údajů apod.

Pro provozování elektronického obchodu je tedy potřeba a věcně ošetřit zatím slabá místa kontraktu. Patří sem:

- ověření totožnosti smluvních stran
- zajištění bezpečnosti přenosu osobních dat a dat představujících obchodní tajemství
- zajištění provedení úhrady
- zajištění bezpečnosti při provádění úhrady
- zajištění bezpečnosti přenosu poskytnutého plnění, je-li poskytováno elektronicky

4.7 MOŽNOSTI ELEKTRONICKÉHO BANKOVNICTVÍ PRO ELEKTRONICKÝ OBCHOD

Banky byly po staletí omezeny při komunikaci s klientem na osobní styk zejména prostřednictvím svých poboček a zástupců. V druhé polovině[9] dvacátého století se však díky prudkému technologickému vývoji tato situace velmi razantně mění a finanční instituce mají k dispozici velkou škálu komunikačních prostředků.

Hnacím motorem změn jsou především 2 základní faktory:

- **úspora nákladů**
- **zatraktivnění služeb pro klienta**

[9] DVOŘÁK, J.- KŘÍŽ, J.- DVOŘÁK, J. *Elektronický obchod.* Skripta VUT v Brně, Fakulta podnikatelská 2005

4.8 PLATEBNÍ KARTY

4.8.1 Požadavky na velikost, ochranné prvky a umístění elektronických údajů

S platební kartou lze provádět v podstatě dvě základní věci – platit za zboží a služby nebo vybírat hotovost z bankomatu. Karta by se vzhledem ke svému názvu měla využívat především k placení a nikoli pro výběry z bankomatu. Pro vlastníka karty je bezpečnější, pohodlnější a hlavně výhodnější platba kartou, jelikož náklady transakce nese obchodník, který dostane o určité procento nižší částku.

Pro obchodníka je platba kartou také výhodnější, i přesto, že si musí pořídit terminál pro operace s platebními kartami. Prvním důvodem je opět bezpečnost, druhou a významnější příčinou, je psychologické chování zákazníka – výzkumy prokázaly a obchodníci již měli možnost v praxi si ověřit, že člověk, který jen podepíše účtenku, nakupuje mnohem více než zákazník platící v hotovosti. Fixní náklady na elektronický terminál i poplatky za transakce by se tak měly obchodníkovi velice rychle vrátit ve zvýšení obratu.

První skupina ochranných prvků spočívá např. v umístění hologramu či kinegramu v ploše platební karty, použití speciálních tiskových technik (klopný efekt, giloš), použití speciálních podtisků, které znemožní přepsání podpisového pole na platební kartě (při přepsání podpisu se např. v podpisovém poli objeví slovo VOID, tj. neplatný), použití prvků viditelných pouze v dopadajícím ultrafialovém či jiném záření a další techniky, použité na[10] základě rozhodnutí emitenta. Zařazovány bývají i utajované prvky, které jsou známy velmi omezenému okruhu osob, zpravidla pouze z okruhu nejvyššího managementu emitenta nebo jeho bezpečnostního pracoviště.

Do skupiny ochranných prvků fakticky patří i potřebné přesné dodržování normovaných rozměrů platebních karet, které je dáno mezinárodním standardem. Základním standardem, který určuje rozměry platební karty, je ISO 7810, přičemž délka karty je stanovena na 85,595 mm, šířka na 53,93 mm a její tloušťka na 0,76 mm. Povolené odchylky se pohybují řádově v setinách milimetrů. Stanoveny jsou i poloměry zakřivení rohů karty, dislokace magnetického proužku, dislokace případně použitého mikročipu a další. Karta odlišných rozměrů není příslušným snímacím zařízením akceptována.

[10] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku) ve znění zákona č. 257/2004Sb.

Do uvedené skupiny ochranných prvků lze volně zařadit i embosované (protlačené, vytlačené) znaky, které mají převážně charakter písmen nebo číslic (ale i dalších znaků, jako jsou různé „hvězdičky“, geometrické obrazce, diakritická znaménka apod.). Embosované znaky jsou v platebních kartách, resp. v jejich nosiči z termoplastické hmoty vytvářeny působením tepelného zdroje, který má tvar požadovaného znaku (vyhřátá raznice potřebného tvaru) a vzhledově jsou tvořeny vystouplými znaky na lícové straně karty a naopak zahloubenými znaky na rubové straně karty. Nosič (základ) platební karty je až na výjimky tvořen termoplastickými hmotami (polyvinylchlorid nebo moderněji polykarbonát), které umožňují svými vlastnostmi při vhodném lokálním zahřátí vytvoření zmíněných znaků. Nosič platební karty může být (a v praxi běžně je) tvořen několika (třemi až šesti) navzájem barevně odlišnými vrstvami, které při vytvoření embosovaných prvků umožňují jejich barevnou odlišnost od převažující barvy podkladu karty (nejčastěji stříbřité, bílé nebo zlatavé barvy). Základní polotovar platební karty je nejčastěji vysekáván s potřebnou přesností z plátu speciální několikavrstvé plastické hmoty, méně často je odléván do formy (již zastaralý způsob zhotovování základu platební karty).

Druhá skupina ochranných prvků platebních karet se týká elektronických údajů, které jsou různými způsoby a na mnohdy značně odlišné technické úrovni v konkrétní platební kartě zakódovány. Z kriminalistického hlediska je tato skupina ochranných prvků obtížněji vyhodnotitelná, protože většinu z nich emitent z pochopitelných důvodů utajuje. V případě potřeby je spolupráce emitenta a kriminalisty nezbytná.

Platí, že elektronické údaje lokalizované na magnetickém proužku, případně nověji na mikročipu, musí být umístěny na přesně vymezeném místě rozměrově standardizované platební karty. Elektronické prvky včetně údajů v nich zakódovaných jsou na polotovar platební karty umisťovány dodatečně, až po vytvoření nosiče karty a umístění ochranných prvků první uvedené skupiny. Individualizace elektronicky kódovaných informací je prováděna až bezprostředně před konkrétním vydáním karty oprávněnému držiteli tzv. nahráním.

4.9 ROZVOJ SPECIFICKÉ STRATEGIE FIRMY PRO ELEKTRONICKÝ OBCHOD

Typickým příkladem prolínání strategií může být např. e-marketing. E-marketing může být součástí jak strategie elektronického obchodu, tak strategie marketingu. Důležitou podmínkou je však zachování konzistence, tzn. že daná problematika je

rozdělena na technickou a logickou část, nebo je zpracována komplexně v rámci jedné z daných strategií. Oblast infrastruktury lze členit do tří základních skupin:

- ***strategické*** - představuje potřebu určit důsledky vlivu technologických změn na podnik a na trh, na kterém tento podnik působí (v podstatě by tedy mělo být cílem podniku sjednocení strategických plánů s možnostmi nejnovějších informačních a komunikačních technologií)
- ***organizační*** - vychází z předpokladu, že na podnik mají vliv různé strategické a technologické změny a ty se projeví primárně v organizaci podniku a jeho struktuře. Z tohoto důvodu je tedy nutné aktualizovat současné procesy tak, aby byly více flexibilnější a vyhovovaly požadovaným změnám
- ***fyzické*** - jedná se o změny v oblastech hardwaru a softwaru

Základem úspěchu bude schopnost podniku přizpůsobovat se změnám. Je třeba propracovat dodržování těchto zásad:

- vytvořit takovou infrastrukturu, která bude flexibilní a vyrovná se s náhlými výraznými změnami
- takto vytvořená infrastruktura by měla být komunikačně vyspělá, tzn. měla by umožnit efektivní komunikaci na všech úrovních
- velmi důležitá je také robustnost, bezpečnost a měřitelnost technologického řešení,
- technologické řešení musí umožňovat komunikaci založenou na dostupných standardech
- velmi důležité bude také ztotožnění se vedení firmy s daným technologickým řešením

Musí být splněny ***základní systémové předpoklady***:

- současné cíle a záměry oblasti elektronického obchodu a jejich soulad s aktuální business strategií
- koncepce a filozofie elektronického obchodu a jejich soulad s aktuální business strategií
- finanční zabezpečení elektronického obchodu
- materiální zabezpečení
- personální zabezpečení
- systém řízení rozvoje elektronického obchodu
- organizace a řízení elektronického obchodu
- aspekt jakosti

- bezpečnost a ochrana elektronického obchodu
- strategické návaznosti

4.9.1 Implementace zvolené strategie elektronického obchodu

Bude velmi složitý proces, jehož úspěch bude závislý na velkém počtu faktorů. Obecně lze konstatovat, že se jedná o proces, v daných podmínkách jedinečný, který má pro fungování podniku zásadní význam. Vrcholovým cílem této fáze je optimální implementace strategie elektronického obchodu. Během zavádění strategie elektronického obchodu by měly být dodržovány určité zásady, mezi které mohou patřit např. následující:

- přehodnocení globální strategie podniku
- nerozvíjet strategii elektronického obchodu nezávisle na obchodní strategii
- použití separátní strategie podle oboru, geografie a kultury
- rovnost interních a externích procesů v průběhu analýzy
- získání podpory vedení všech zaměstnanců
- změny obchodního modelu

4.9.2 Klíčové faktory

Elektronické obchodování není jednoduchou záležitostí. Klíčové faktory umožní implementaci úspěšné strategie lze shrnout, podle literatury, do následujících deseti bodů:

- **Získat odbyt**
- **Používat tzv. „click-and-mortar“ strategii pokud je to možné**
- **Integrovat nákupní zkušenosti**
- **Plánovat řízení obsahu, cen, zásob, plnění, podpory, plateb, vrácení zboží a bezpečnosti**

Obsah – obsah elektronického obchodu musí být často aktualizován

Ceny - pokud prodáváme zboží přímo poprvé, mohou vzniknou problémy s distributory nebo maloobchodníky, kteří nebudou souhlasit s naší nižší cenou. Nabízíme prodej ve více měnách? Pokud ano, tak v jakých?

Řízení zásob – užíváme stejnou základnu zásob pro prodej on-line jako v případě fyzického prodeje? Jestliže ano, je třeba mít integrovaný systém řízení zásob.

Plnění – precizní informace o stavu objednávky jsou nutností. Každý zákazník by měl mít přístup k informacím o své objednávce a jejím průběhu až po moment doručení. Jestliže jsme dosud neprodávali pomocí běžných objednávek, musíme vytvořit plán balení a plnění. Ten může být dost nákladný a vyžaduje pečlivé řízení. Jestliže nebudeme

dodávat z nákladových nebo jiných důvodů do určitých zemí, je třeba to na webových stránkách zřetelně vyznačit.

Platby – jak budou lidé platit? Jaké platební karty budeme akceptovat? Jak budeme řešit podvody?

Podpora – jak budeme podporovat produkty prodávané on-line? Musíme mít plán pro oblast podpory na webu, abychom mohli zodpovědět jednoduché otázky zákazníků. Budeme nabízet také telefonickou podporu, či podporu prostřednictvím e-mailu?

Zabezpečení – zabezpečení je základní problematikou strategie elektronického obchodu, neboť podvody a různé neoprávněné přístupy či nabourávání do systémů budou stále častější.

- **Vyvinout uživatelsky přátelský nákupní postup**
- **Zvážit oblast působení**
- **Zvážit užití systémů CRM**
- **Ujistit se, že kupujeme správný software**
- **Ujistit se, že máme tým na svém místě**
- **Nebudeme-li elektronický obchod podporovat, zákazníci sami nepřijdou**

Aby bylo dosaženo „optimálnosti“ musí být splněna celá řada [11]podmínek a požadavků, mezi které patří zejména:

- **Kvalita návrhu strategie elektronického obchodu**
- **Dostupnost zdrojů**
- **Určení a přiřazování úkolů**
- **Vymezení intervenční oblasti**

4.9.3 Vymezení informačního zabezpečení elektronického obchodování

Pro činnost zpracování informace je nezbytné získávání informací:

- ***Registry orgánů veřejné správy***
  - Registr ekonomických subjektů
  - Obchodní rejstřík
  - Registr živnostenského podnikání
  - Evidence plátců daní
  - Administrativní registr ekonomických subjektů, katastr nemovitostí

- ***Další veřejnoprávní zdroje***
- ***Ostatní veřejné zdroje informací***
- ***Mezinárodní zdroje***
- ***Vlastní získávání informací***

[11]DVOŘÁK, J.- KŘÍŽ, J.- DVOŘÁK, J. *Elektronický obchod.* Skripta VUT v Brně, Fakulta podnikatelská 2005

Ochrana informací může být strukturována:

- ***utajované skutečnosti***
  - personální bezpečnost
  - administrativní bezpečnost
  - objektová bezpečnost
  - technická bezpečnost
  - bezpečnost informačních systémů
  - kryptografická ochrana
  - průmyslová bezpečnost

Ochrana důvěrných informací:

- citlivé informace
- informace pro vnitřní potřebu
- veřejné informace

Obsahem ***bezpečnostní politiky*** informačního systému organizace jsou:

- definice bezpečnosti informací, její cíle, rozsah a důležitost
- prohlášení vedení organizace o záměru podporovat cíle a principy bezpečnosti informací, výklad bezpečnostních zásad, principů, standardů a požadavků
- stanovení odpovědností
- odkazy na dokumentaci

4.9.4 Informační a komunikační technologie

Odevzdáním řízení společnosti do rukou výpočetní techniky a nástupem celosvětové sítě jsme se nezbavili vlastní zranitelnosti. Ba právě naopak. Scénáře scifi příběhů se stávají každodenní realitou. Osobní anonymita je často pouze zdánlivá, důležitá data při neopatrnosti (často i při opatrnosti) zase snadno napadnutelná a zcizitelná. Informační a komunikační technologie (dále ICT) jsou nasazeny snad do všech oblastí společenského a soukromého života – ekonomiky, veřejné správy, armády, průmyslu zdravotnictví, vzdělání atd. Informace, které se týkají těchto a dalších oblastí jsou implementovány do informačních systémů a jsou pro jednotlivé subjekty vysoce ceněnou hodnotou - často jde o velmi citlivé údaje týkající se obchodních informací atd. Veškeré informační procesy jsou digitalizovány, dochází ke snížení prostorového a časového omezení a zvýšení přístupu k různorodým informacím. **Digitální informace** jsou univerzálně použitelné, duplikovatelné a transformovatelné, a tudíž i velmi lehce zneužitelné. Za tím vším stojí **ICT**, které jsou jednak nezměrným přínosem pro lidskou společnost, ale v případě zneužití jsou zároveň velmi nebezpečnou zbraní. Jinými slovy, technologický pokrok dává vzniknout rozvoji kriminálnímu. Tempo technologického pokroku je nezadržitelné (Mooreův zákon) [1] a s ním i vynalézavost pachatelů elektronické informační

kriminality. Zvyšuje se (do jisté míry) počítačová gramotnost uživatelů a přístup k internetu má díky nízkým cenovým nabídkám téměř každý. Všechny tyto aspekty prohlubují možnosti zneužití ICT. V souvislosti s rozšiřováním ICT do celého světa je nutné zmínit jejich nevyvážené pokrytí a vznik tzv. **digitální propasti** (digital divide). Rozvojové země s minimální technologickou úrovní se pak mohou stát výhodnou základnou nebo přestupní stanicí kybernetických útoků. V takovýchto zemích se předpokládá nízká, popř. nulová úroveň legislativy, což je pochopitelně pro útočníky neodolatelným lákadlem. Elektronická informační kriminalita (dále EIK) se však dotýká velmi významným způsobem i jednotlivců. Ukradená data, ať už méně či více sofistikovaným způsobem, jsou dále využívána k podvodným transakcím (e-commerce, e-banking), internetovému obtěžování atd. A nejde jen o útoky na data, jde také o velmi významnou oblast ochrany autorských práv, která jsou v prostředí internetu masivně porušována.

V českém prostředí se nejčastěji setkáváme s termínem **počítačová kriminalita**, kterou můžeme chápat jako páchání trestné činnosti, v níž figuruje počítač jako souhrn technického a programového vybavení včetně dat, či pouze některý z komponentů počítače, případně více počítačů propojených do počítačové sítě. Tento nový obor zločinnosti vznikl v okamžiku, kdy se počítače začaly měnit z matematických strojů v původním slova smyslu v mnohoúčelově použitelná zařízení, schopná převzít nejrůznější agendu a kdy někdo přišel na „skvělý“ nápad, že modifikací programu nebo dat zpracovávaných počítačem může dosáhnout účinku, který způsobí někomu škodu či jinému neoprávněný prospěch. Současně se objevil také počítač jako zločinný nástroj, neboť někdo úplně jiný zjistil, jak snadno lze některé trestné činy páchat s tak skvělým pomocníkem. Ale samozřejmě ze všeho nejdříve se počítače staly předmětem klasických kriminálních útoků, směřujících proti nim coby věcem movitým – krádeží, neoprávněného užívání, poškozování cizí věci atd.;

Počítač může být jak **předmětem**, tak **nástrojem trestné činnosti**. Vzhledem k tomu, že delikty v této oblasti jsou páchány s využitím moderních IT, se již delší dobu hovoří o **kriminalitě informační** či **informatické**. SMEJKAL[12] ji definuje jako kriminalitu, která by mohla zahrnovat trestněprávní, autorskoprávní a občanskoprávní (osobnostní) aspekty, prováděné veškerými technologiemi pro zpracování a přenos informací. V zahraničí jsou ustáleny termíny **computer crime, high-tech crime** či **cybercrime** [2], tedy doslovně kriminalita kybernetická. Rada Evropy zavedla pojem **„computer related crime“**, který

[12] SMEJKAL, V. *Informační a počítačová kriminalita v České republice* [online]. [cit. 2004-12-16]

definuje jako nelegální a nemorální jednání zahrnující užití nebo změnu dat získaných prostřednictvím výpočetní techniky.

O EIK můžeme jednoduše říci, že jde o určitou modifikaci standardních trestných činů s řadou výrazných charakteristik, které ji od kriminality klasické odlišují (absence násilí, zbraní či fyzické újmy na zdraví). U klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, kdežto trestný čin v kyberprostoru kriminality může být spáchán v několika tisícinách sekundy a pachatel ani nemusí být přímo na místě činu. Další významnou charakteristikou jsou poměrně značné ztráty, ať již přímo v podobě finančních částek, nebo v rámci zneužití získaných údajů. EIK také provází určitá diskrétnost trestné činnosti. Z uvedeného vyplývá, proč bývá tato kriminalita pro svou povahu označována jako kriminalita "bílých límečků". [13]

4.9.5 Historie a současnost elektronického obchodu

Vznik EIK vyplývá z historického vývoje výpočetní techniky, resp. ICT. Odrazovým můstkem se stalo masové využívání osobních počítačů a jejich propojování do sítí, především internetu. Jeho existence znamená zásadní zlom [14] nejen do kvality, ale bohužel i do kvantity zločinů týkající se EIK. Vývoj v **České republice** je kvůli opožděnému zavedení IT poněkud odlišný. K prvním trestným činům v této oblasti dochází až na konci 80. let, kdy se v tehdejších československých domácnostech začaly objevovat první počítače.

Nynější oddělení se historicky formovalo poměrně vlažně. Na začátku 90. let se policie v oblasti trestné činnosti využívající IT omezovala pouze na znalecká zkoumání v Kriminalistickém ústavu Praha, která se postupně rozšířila na krajské správy.

Absence výkonné části byla vyřešena v roce 1998, kdy vznik specializované skupiny na Policejním prezidiu ČR podnítila potřeba vytvoření operativní a vyšetřovací složky. Její náplní se zpočátku stala oblast softwarového pirátství, postupně však byla přenesena na základní útvary služby kriminální policie a vyšetřování (ÚSKPV) na úrovni okresů a krajů. ÚSKPV nyní plní v souvislosti se softwarovým pirátstvím spíše koordinační a metodickou úlohu.

Na začátku roku 2008 došlo ke změně struktury a vzniku nového pojetí oddělení informační kriminality. Plánuje se vytvoření specializovaných míst operativních detektivů na útvarech s republikovou působností a současně na jednotlivých krajských správách

[13] KŘÍŽ, L. *X-vize budoucí bezpečnosti* [online]. 1.1.2006
[14] Bibliografický záznam původní práce: PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita*

Policie ČR. Jako první vzniklo 1. května 2005 pracoviště na Policii ČR, Správě hl. m. Prahy.

První sálový počítač - ENIAC - byl sestrojen roku 1946 na Pensylvánské univerzitě. Na přelomu 50. a 60. let byly tyto počítače využívány v mnoha společnostech a univerzitách. Údržba těchto strojů byla velmi finančně a časově náročná, proto docházelo k zásahům do programů, tzv. **„hacks“**, které měly zefektivnit chod operačního systému (dále OS) či aplikací. První generací hackerů byla v 60. letech identifikována skupina studentů MIT [3], která měla k těmto počítačům přístup. Mezi význačné osobnosti tohoto období patří Richard Stallman, zakladatel *Free Software Foundation* [4].

V 70. letech se zrodilo zneužívání telefonních linek. Touto činností se zabývají tzv. **phreakers** (telefandové). Roku 1971 počítačový nadšenec **John Draper** (dříve známý pod jménem Captain Crunch) objevil, že plastová píšťalka dodávaná k populárním cereáliím vydává zvuk na frekvenci 2600 Hz. Tento kód způsobil odblokování telefonní sítě AT&T a umožňoval hovory zdarma. (Dnes se „Captain Crunch“ staví na druhou stranu barikády, roku 2002 vyvinul specializovaný počítač *CrunchBOX*, který má ochránit uživatelská data i celou síť.) Roku 1975 S. Wozniak a S. Jobs (zakladatelé firmy *Apple Computers*) začali vyrábět tzv. **„blue boxes“(BBS)**, zařízení založené na Draperově objevu. Na konci 70. let došlo k důležité události, a to sestrojení prvního **BBS** [5], díky němuž se uživatelé vybavení počítačem s telefonní linkou mohli stát součástí kyberprostoru.

K rozšíření těchto technologií došlo až s představením osobních počítačů firmou IBM, které s sebou přinesly jednoduchý operační systém, binární kompatibilitu programů a hlavně masovou výměnu dat a programů mezi uživateli. V **České republice** se objevují ojediněle trestné činy v podobě sabotáží podnikových záznamů či technického vybavení.

V 80. letech byly počítače díky IBM čím dál více propojovány do sítí - tak došlo k rozšíření předchůdce dnešního internetu v podobě systému BBS. Jednalo se většinou o servery s textovým rozhraním, na které se připojovalo přímo volbou čísla, zprostředkování přístupu pomocí ISP přišlo až později.[15] Z tohoto undergroundu vzešla hackerská legenda **„Legion of Doom“**, která nebyla nikdy organizovaným společenstvím

[15] LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista.* 1998, č. 3, s. 3-15

osob, neměla stálé členy, hierarchii ani nic podobného. Jejich nepostradatelnou činností bylo publikování článků v různých undergroundových médiích. Nejznámějším časopisem se stal Phrack, který byl nepřijemný státním orgánům. Ke konci 80. let došlo k enormnímu rozšíření hackerských skupin. S rokem 1982 přichází na svět nové médium pro záznam digitálních dat **CD-ROM** s kapacitou 650 MB, což umožnilo kvalitativně zvýšit pirátské aktivity. V roce 1984 začal Eric Corley publikovat časopis *2600: The Hacker Quarterly*, který se stal předním zdrojem informací pro hacking a který dosud vychází. V roce 1987 se na Delawarské univerzitě objevil **první virus**, který nezpůsobil žádné trvalé poškození, pouze drobné systémové chyby. Známým pachatelem tohoto desetiletí byl také vysokoškolský student z Cornellovy univerzity **Robert Morris Jr.**, který poslal roku 1988 do světa svůj virus *InternetWorm*, a **Kevin Mitnick** [6], který je znám především svým útokem na počítače společnosti Digital Equipment. Téhož roku také došlo ke slavné počítačové krádeži v chicagské First National Bank, která tak přišla o 70 milionů dolarů. V **českém prostředí** dochází k dokladovým deliktům ve formě změn dat v počítači vedoucím k obohacení pachatele či k neoprávněnému užívání počítačů.

Pro 90. léta je charakteristické masové rozšíření osobních počítačů, zejména s operačním systémem Microsoft Windows (dále jen OS MS Windows), čímž vzrůstá i vývoj příslušného softwaru (dále jen SW). Rozvoj počítačových sítí, především **internetu**, nese své důsledky v narůstající trestné činnosti. Internet se z akademických kruhů dostává do komerční sféry a stává se tak velmi lákavou příležitostí k páchání nelegálních aktivit, které exponenciálně narůstají. Disketové mechaniky nahrazují CD-ROMy, vznikají **anonymní FTP servery** a začíná se rozvíjet **globální počítačová kriminalita**. Z typického pachatele předchozích etap, tedy počítačového nadšence, se stává chladný profesionál, jehož cílem je vlastní obohacení. Fenoménem konce 90. let se do jisté míry stávají **P2P sítě** [7]. Roku 1990 byli zatčeni čtyři členové **Legion of Doom** za krádež technické specifikace společnosti *BellSouth*, popisující záchranný systém 911, kterou ve zkrácené verzi publikoval Knight Lighting v časopise *Phrack*. V témže roce dochází k historické události známé pod jménem **„Operace Sundevil“**. Šlo o celostátní policejní razii v USA, která měla za cíl zadržet elektronické podvodníky, odpovědné za krádeže kreditních karet a zneužívání telefonních kódů. Operace měla[16] především odstrašující charakter a vyvolala tak otázky ochrany svobody projevu a občanských práv v kyberprostoru. Došlo k založení *Electronic Frontier Foundation* [8], neziskové společnosti zabývající se právy uživatelů digitálních technologií. Roku 1991 se **Kevin Poulen** s dvěma dalšími hackery naboural do telefonních linek kalifornské rozhlasové

[16] Bibliografický záznam původní práce: PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita*

stanice a zmanipuloval tak reklamní soutěž. V roce 1994 pronikli dva hackeři „Data Stream“ a „Kuji“ do několika stovek počítačových sítí, včetně *NASA* a *Korejského jaderného výzkumného institutu*. V roce 1995 ruský počítačový nadšenec **Vladimir Levin** pronikl do počítačové sítě americké banky *Citibank* a převedl na své bankovní účty poměrně vysoké finanční částky. V roce 1996 se proslavil americký hacker **Timothy Lloyd**, který pomocí šestiřádkového kódu způsobil společnosti *Omega Engineering* škodu za více než 10 milionů dolarů. Tento kód smazal veškerý důležitý software a Llyodův případ se stal jedním z nejznámějších napadení společnosti vlastním zaměstnancem. Roku 1999 **David Smith** vytvořil ***virus Melissa***, který způsobil globální ohrožení počítačů. Po celém světě nakazil a zlikvidoval přes 300 počítačových firemních sítí. Celková škoda byla vyčíslena na 400 milionů dolarů. Roku 1999 byla společností RIAA podána žaloba na systém pro sdílení hudby **Napster**. Výsledkem bylo zablokování skladeb chráněných autorským právem (dále AP), a tím pádem odliv uživatelů na jiné sítě P2P. Napster byl nakonec zrušen a odkoupen firmou *Bertelsmann* (součástí je nahrávací studio BMG). Nyní nabízí legální prodej hudby přes internet. Na počátku 90. let v **České republice** stály v popředí burzy s nelegálními hudebními či filmovými nahrávkami a pochopitelně nelegálním SW. Podle BSA [9] dosahovala míra používání nelegálního SW až 80 %. Situace se začala pozvolna měnit s nárůstem kupní síly obyvatelstva a šířenou osvětou o nelegálním SW (v roce 2003 míra softwarového pirátství klesla na 40 %). Dále u nás dochází zejména ke zneužívání osobních dat, šíření pornografie a internetovým podvodům typu letadla [10] či bankovním podvodům (v letech 1992-2000 došlo k 13 zveřejněným bankovním počítačovým zločinům, všechny případy se týkaly neoprávněné manipulace s bankovními záznamy). V roce 1996 se na českém a slovenském internetu objevují hackerské skupiny *CzERT* a *Binary Division*, které se specializovaly na pozměňování webů (ukázky na www.hysteria.sk/hacked).

V současnosti je naše společnost stále více závislá na počítačích a počítačových sítích. Počet uživatelů internetu neustále roste, v České republice během let 2000-2005 **vzrostl počet uživatelů** o celých **170 %** [11]. Rozvoj internetu změnil chápání autorského díla (vznik sítí P2P), internet se také stále více stává nástrojem **organizovaného zločinu**. Počítačoví piráti se spojují do skupin, vzniká tzv. **warez**. Nelegální SW se šíří prostřednictvím anonymních FTP serverů či decentralizovaných výměnných systémů typu peer-to-peer. Začínají se také objevovat věrohodné padělky autorských děl hudebních, filmových či software. Čím dál častěji se objevují typy útoků jako **spamming,**

phishing, pharming, rozesílání malware [12] (dle statistik McAfee [17]bylo zaznamenáno téměř každý měsíc 1500 škodlivých virů) či **spyware** [13]. Novým typem útoku se stává zaheslování souborů uložených na počítači na dálku a následné výkupné za SW - tzv. **ransomware**. V roce 2000 hacker **MafiaBoy** napadl významné webové servery jako *Yahoo, eBay či Amazon* a získal tak přístup k 75 počítačům v 52 sítích a spouštěl na nich DoS útoky [14]. V témže roce spatřil světlo světa vir ***„I love you“***, který způsobil škodu asi 10 miliard dolarů. Jeho autorem byl filipínský student **Onel DeGuzman**, který vzhledem k neexistenci příslušné filipínské legislativy nemohl být odsouzen. V letech 2000-2001 probíhal soudní spor mezi internetovým portálem ***Yahoo*** a francouzskou ligou proti rasismu ***LICRA***. *LICRA* žalovala *Yahoo* za propagaci nacismu, neboť přes aukční stránky portálu byly přístupné nacistické materiály. V roce 2001 došlo k zatčení ruského softwarového inženýra **Dmitryho Sklyarova** z firmy *ElcomSoft*, který porušil AP. Podařilo se mu prolomit ochranu elektronických knih Adobe ve formátu PDF. *ElcomSoft* nabízí utilitu *Advanced eBook Processor*, která převádí elektronické knihy z chráněného formátu *Adobe eBook* na nechráněný formát PDF. Roku 2002 byl zatčen **Gary McKinnon** z Velké Británie, který pronikl do více než 90 počítačů americké armády ve Velké Británii. V roce 2005 došlo k největšímu útoku na bezpečnost bankovních dat - kvůli nedostatečným směrnicím a nařízením společnosti *MasterCard* bylo ohroženo až 40 milionů kreditních karet. Tentýž rok se na internetu objevily nové verze virů. V modifikované variantě zaútočil několik let starý ***vir Sober***, který je součástí e-mailu tvářícího se, že jeho odesílatelem je FBI. ***Červ Mytob*** se snaží příjemce přesvědčit, že e-mail pochází od poskytovatele internetového připojení.

V **České republice** dochází v roce 2000 asi k nejznámějšímu případu porušení AP. Počítačová firma *Mironet* byla obviněna z instalace nelegálního software. Po neúspěšné policejní prohlídce případ utichl, *Mironet* však nakonec žaloval firmu Microsoft, která několik let vyvíjela tlak na instalace OS Windows, a tak upadla v podezření z policejního udání. Mezi další případy můžeme zařadit umístění pirátských kopií českých filmů na internet, bankovní podvody, krádeže citlivých údajů a jejich následný prodej či e-mailové hrozby. Ani naše republika není ušetřena phishingových útoků.

---

[17]MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. 97 s. ISBN 80-7226-419-2

4.9.6 Členění pachatelů z hlediska jejich vztahu k informacím

Nové technologie vytvořily živnou půdu pro podvodníky, kteří začali využívat počítačů pro „klasickou“ trestnou činnost, nyní ovšem snáze proveditelnou. Hlavní oblastí, která představuje těžiště hospodářské trestné činnosti v ČR, jsou podvody. Klasické podvody podle § 250 Trestního zákona („Kdo ke škodě cizího majetku sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, ..“) byly nyní zdokonaleny pomocí počítačů, případně se objevily zcela nové druhy podvodů.

Sjednocujícím kritériem takovýchto jednání je vždy více méně využití něčího omylu ve svůj prospěch. Psychologickou stránku vztahu počítač – člověk shrneme z pohledu našich zkušeností.

Na rozdíl od klasických manipulací s „papírovými“ doklady má manipulace s počítačovými daty pro pachatele několik výhod:

1) vymazání či přemazání údaje na magnetickém médiu je podstatně snazší a nezanechává prakticky žádné stopy
2) člověk (zaměstnanec, auditor, zákazník apod.) z psychologického hlediska považuje výsledky z počítače za a priori správné a více jim (byť podvědomě) důvěřuje
3) systém zpracování dat je natolik složitý, že málokdo má přehled o všech aspektech, procedurách, postupech a mechanismech, jež jsou používány a kontrola toho, co se odehrává ve výpočetním systému je velmi obtížná
4) zjištění stavu informačního systému v určitém, mnohdy časově vzdáleném okamžiku a prokázání odpovědnosti určité osoby za provedení operací v tomto IS je obtížné, ne-li nemožné
5) objem zpracovaných, resp. přenášených dat je velmi velký
6) lehkost provádění operací s počítačovými (virtuálními) daty oproti reálnému životu; ukrást někomu z kapsy peněženku je výrazně obtížnější než napsat příkazový řádek na počítači – alespoň pro kvalifikovaného programátora
7) morální aspekty jsou ve virtuálním světě poněkud potlačeny – nechceme vytvářet atmosféru boje proti počítačovým hrám, ale je nepochybné, že je výrazně lehčí zlikvidovat někoho stisknutím tlačítka „Enter“ kdesi na druhém konci zeměkoule, nežli se ozbrojit olověnou trubkou a za stejným účelem se vydat do krčského lesíka. Podobně – abychom nebyli obviněni z nadsázky – daleko snadněji lze

kliknutím myši odcizit autorské dílo, nežli kdyby jej pachatel musel řádek po řádce přepisovat.

Pachatele můžeme dělit také z hlediska jejich **vztahu k informacím**, a to na:

- **Amatéry,** kam bychom zařadili hackery, crackery, neúspěšné kritiky a mstitele. Jde o osoby pronikající náhodně nebo cílevědomě do informačních systémů tak, že vyhledávají zranitelná místa. Jejich cíle nebo motivace jsou různé.
- **Profesionály,** kam by patřili pracovníci speciálních tajných služeb, detektivové, žurnalisté, podnikatelé, specialisté informatici, softwaroví piráti či teroristé (zvláštní skupina organizovaného zločinu). [18]

Někteří pachatelé provádějí trestnou činnost samostatně, ale ve většině případů jde o sdružování a spolupráci více osob, které se formují do určitých skupin. Jednotliví členové se většinou ani osobně neznají, neboť veškerá komunikace probíhá elektronicky. Vztahy mezi undergroundovými skupinami, zabývajícími se touto trestnou činností, jsou poměrně spletité.

Význam označení **hacker** [15] prodělal v průběhu let pozoruhodný vývoj. Zatímco dříve bylo synonymem pro člověka, ke kterému se vzhlíží s úctou, dnes jej většina lidí považuje za označení počítačového kriminálníka. Termín se objevil mezi radioamatéry již v 50. letech, o desetiletí později byl použit komunitou hackerů. Obecně můžeme říci, že hacker je člověk nadšený programováním, kterého baví zkoumat detaily a způsoby využití systémů; překonávání překážek tvořivým způsobem je pro něj výzvou. Musíme tedy zdůraznit, že činnost pravého hackera spočívá v **pronikání do ochraňovaných systémů** s cílem **prokázat své schopnosti** a **kvality bez zájmu získat informace** či **narušit systém**. Podstatné je překonávání ochranných bariér, což je považováno za zábavu, dobrodružství. Pro opravdové hackery je typické jejich sociální chování, používaný jazyk, uznávání morálních hodnot a samozřejmě provádění samotného hackingu. Pojem **hacking** označuje činnosti, které pravý hacker provádí a kterými získává uznání a respekt - získání a zpřístupnění zdrojového kódu programů, odhalení slabin informačního systému a zpřístupnění příslušných informací, publikování užitečných informací na internetu, pomoc při administrativě a provozu diskuzních skupin, seznamů,

[18] KŘÍŽ, L. *X-vize budoucí bezpečnosti* [online]. 1.1.2006 [cit. 2006-02-10]

archivů atd., pomoc při testování nových programů – tzv. beta verze či propagace hackerské kultury.[19]

Pro zajímavost můžeme zmínit, že hacking, který **není** prováděn tak, aby způsobil někomu jinému škodu či jinou újmu nebo sobě či jinému neoprávněný prospěch, není kvalifikován jako trestný čin, a tudíž **není postižitelný**. Pro doplnění je ještě nutné uvést pojem **hactivismus**, který představuje politicky motivované napadání internetových stránek. V důsledku různých medializovaných kauz průniků do sítí se výraz „hacker" vžil jako nálepka pro vandalství, poškozování informačních a komunikačních systémů.

Označení **cracker** se objevilo v souvislosti s pojmem **crack**, který představuje narušení zabezpečení ochrany a integrity programu nebo systému. Podle jednoho pohledu jde o osoby schopné **prolomit kód** určitého SW a umožnit tak jeho nelegální kopírování, z jiného hlediska jde o osoby, které **pronikají do počítačových systému s úmyslem jejich poškození. Cracking** [16] je činnost, kdy dojde k narušení informačního systému zvenčí (prolomení ochrany). Cracker zpravidla nepracuje sám, ale ve skupinách. Členové skupiny bývají hierarchicky rozděleni, každý má na starosti konkrétní činnost. Skupiny bývají tématicky specializované na herní oblasti, weby a aplikace. Mezi skupinami panuje poměrně vysoká soutěživost, své úspěchy pečlivě dokumentují a zpravidla i zpřístupňují na internetu. [20]Crackeři se sami často považují za hackery, avšak jejich znalosti informačních systémů, internetových protokolů a programování nejsou na tak vysoké úrovni jako u hackerů. Crackeři používají k průniku do informačních systémů především zveřejněné slabiny, na které ještě administrátoři nezareagovali. Zásadní rozdíl, odlišující tyto patogenní osobnosti od hackerů, spočívá v pronikání do systémů s cílem data získat a následně zneužít ve vlastní prospěch. K těmto charakteristikám můžeme ještě přiřadit potěšení z destrukce systému.

Pro získání celkového přehledu osob pohybujících se v digitálním undergroundu jsou uvedeny další pojmy:

- **samuraj** – útočník, který pronikne do systému, avšak následně správci oznámí bezpečnostní nedostatky a poskytne mu konkrétní rady
- **script-kiddies** – začínající útočníci s průměrnými znalostmi, kteří dokáží na internetu najít kód a mírně ho upravit, např. pro spuštění nové varianty viru (převážně využívají nástroje vytvořené jinými útočníky - skripty)

[19] SVETLÍK, M. Informační bezpečnost : část 1-4. *Softwarové noviny*. 2002, č. 2-5
[20] PŘIBYL, T. Po phishingu přichází pharming. *Computerworld.* 2005, č. 27, s. 28-29

- **packet monkeys** – nezkušení uživatelé, kteří provádí DoS útoky či jiné útoky nevyžadující prolomení ochrany, opět za použití utilit vytvořených jinými
- **phreaker/phracker** – útočník, který proniká a zneužívá telefonních sítí
- **phisher** – útočník, který vytváří identické webové stránky většinou různých finančních institucí a poté ukradne a zneužije citlivé údaje uživatelů, kteří je zadají v domnění, že jde o oficiální stránky instituce
- **knacker** – útočníci, který odstraňují ochranný kód programů za účelem jeho volného používání
- **looser/lamer** – uživatelé neznalí prostředí IT

V literatuře zahraničních autorů [21] se můžeme také setkat s pojmy:

- **white hats** – tzv. „hodní“ hackeři, kteří nezpůsobují žádné škody a upozorňují administrátory systémů na objevené bezpečnostní chyby, někdy jsou také označování jako „ethical hackers“ – jde tedy o hackery v pravém slova smyslu
- **black hats** – hackeři s kriminálními motivy, účelem je vlastní obohacení – jde tedy o tzv. crackery
- **grey hats** – šedá zóna hackerů stojící na pomezí mezi předchozími typy, typické je pro ně zveřejňování bezpečnostních děr, tzv. exploitů v internetu za účelem růstu úrovně bezpečnosti systémů (výše uvedený samuraj)
- **elite** – hackeři proslavení nejlegendárnějšími kousky

4.9.7 Zásady informační bezpečnosti

Informační bezpečnost (dále IB) můžeme definovat jako vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti ICT pro zajištění dostupnosti, důvěryhodnosti a integrity informací. [22]Informační bezpečnost se stává samostatným multidisciplinárním oborem, měla by tedy být chápána jako komplexní a dynamická záležitost a vzhledem k neustálému technologickému vývoji by mělo být její budování trvalým procesem. Bezpečnost se nedá zúžit pouze na IS nebo ICT, musí se řešit všechny aspekty včetně organizačních procedur a chování jednotlivců. K informacím, které jsou nejčastěji v ohrožení, patří osobní data

[21] TOLAR, O. *Policie je krátká na weby popírající holocaust* [online]. 22.2.2006 [cit. 2006-02-26]
[22] SMEJKAL, V. *Právo informačních a telekomunikačních systémů.* Praha : C. H. Beck, 2004. xxx, 770 s. ISBN 80-7179-765-0

občanů a hospodářsky využitelné údaje. Ochrana soukromí je dána Ústavou ČR a Listinou základních práv a svobod. **Ochrana osobních údajů** v prostředí informačních systémů byla původně ustanovena zákonem č. 256/1992 Sb., který se však ukázal nevyhovujícím a stal se terčem kritiky. Nedostatky měl odstranit zákon č. **101/2000 Sb.** , o ochraně osobních údajů. Ten upravuje ochranu osobních údajů, práva a povinnosti vznikající při jejich zpracování, sankce za porušení. Vztahuje se na osobní údaje zpracovávané státními orgány, orgány veřejné správy, fyzickými či právnickými osobami. Elektronické zpracování občanských osobních údajů je dnes zcela běžnou činností, a proto je jejich právní úprava nezbytná.

S postupující globalizací informační společnosti a vývojem ICT jsou osobní údaje čím dál cennější, ale zároveň také zranitelnější. Získané soubory dat lze velmi dobře prodat, ale také propojit s kteroukoli jinou databází - což může způsobit vytvoření celistvého obrázku o uživateli, jeho zájmech, majetku atd. Spousta citlivých údajů - jako čísla kreditních karet, mobilních telefonů - umožňuje najít také oblíbený vyhledávač **Google**, který je sbírá, a je tak bránou k celým databázím přístupových jmen a hesel.

Cílem řešení IB je vytvoření **maximální ochrany** před možnými útoky s **minimálními náklady**. [23] Za tímto účelem čím dál více specializovaných firem nabízí podnikům systémy řízení informační bezpečnosti, tzv. ISMS (Information Security Management System). Zavádění ISMS je prováděno podle modelu PDCA (Plan – Do – Check – Act), který je naznačen v obr. č. 1.

Obrázek 1 **Model PDCA – teorie bezpečnosti**

[zdroj] 24.

[23] F.S.C. *Zavedení systému řízení informační bezpečnosti – ISMS.* [online]. [cit. 2006-02-12]

Teorie bezpečnosti informací popisuje tři základní atributy nezbytné k zabezpečení informací.

- **důvěryhodnost** – zajištění toho, že informace je dostupná pouze osobám s autorizovaným přístupem
- **integrita** – zabezpečení přesnosti a kompletnosti informací a metod zpracování
- **dostupnost** - zajištění toho, že informace a s nimi spjatá aktiva jsou dostupné autorizovaným uživatelům podle jejich potřeby

K těmto třem základním požadavkům bychom mohli ještě doplnit:

- **zodpovědnost** – privilegování individuální zodpovědnosti
- **spolehlivost** - zajištění konzistence chování a výsledků

V podstatě jde tedy o to, aby relevantní informace byly dostupné oprávněným osobám pouze v nezbytně nutném rozsahu a jenom tehdy, kdy je to potřebné.

Budování IB obnáší zajištění interních i externích lidských zdrojů, vyhrazení finančních prostředků, zodpovědnost a v neposlední řadě smíření se s faktem, že řešení bezpečnosti je nikdy nekončící proces. **Podnětem** k budování IB jsou **bezpečnostní rizika** (ohrožující data a informace), která mohou pocházet z různých zdrojů. Dle určitého zjednodušení rozeznáváme rizika personální, administrativní a technická. V první řadě zde selhává **personální faktor**, ke kterému se přidávají faktory obvykle též spočívající v personální rovině, kdy zaměstnanci zodpovědní za bezpečnost a výpočetní techniku nesplnili své povinnosti nebo podcenili hrozící nebezpečí. Z hlediska možného zneužití informací je nejslabším článkem v celém informačním procesu člověk. Personální rizika jsou ovlivněna životními postoji, psychikou člověka, zainteresováním na pracovním úkolu a v podstatě přístupem k celé problematice. V případě úmyslného promyšleného útoku vychází pachatel ze znalosti vnitřního systému, disponuje určitou úrovní oprávnění přístupu a nic mu, snad kromě svědomí, nebrání k provedení útoku. Proto je třeba implementovat dle konkrétní situace účinná **technologická** (šifrování síťové komunikace, používání antivirových a antispywarových programů, pravidelné provádění aktualizací, implementace firewallu apod.) a **organizační** opatření (vypracování bezpečnostních pravidel, směrnice, oddělení intranetu od internetu, časově rozlišené přístupy, certifikace systémů, sofistikovaná a silná autentizace - např. pomocí biometrie, používání silných hesel atd.).

Zpracování bezpečnostní politiky je povinné podle zákona č. **412/2005 Sb.**, o ochraně utajovaných informací, a zákona č. **353/1999 Sb.**, o prevenci závažných havárií. IBP chápeme jako **programový úkol**, který:

- definuje hlavní cíle při ochraně informací
- stanoví způsob řešení bezpečnosti (budování ISMS)
- určuje pravomoci a odpovědnosti za budovaný ISMS

Vytvořením IBP však proces budování bezpečnosti nekončí, to nejdůležitější, a sice **implementace** a **následná kontrola**, je na privilegovaných zodpovědných osobách. Zaměstnanci by měli být řádně proškolováni (praktické ukázky, ne jen nudná teorie), popř. by měly být prověřovány jejich znalosti. Proces „učení“ by neměl být jednorázovou akcí, ale měl by být prováděn průběžně, ruku v ruce s vývojem ICT a dle aktuálnosti problémů. Další významnou aktivitou je provádění **monitoringu** a získávání zpětné vazby, na základě kterých se situace může efektivně vyvíjet dál. Vrcholem zavádění IB by měla být **certifikace celého ISMS**.

4.9.8 Elektronická informační kriminalita a její členění

EIK, jak již bylo naznačeno v úvodu, spočívá ve zneužití ICT k páchání trestných činů. Jedním z nejrychleji se vyvíjejících typů informačního zločinu v kyberprostoru je krádež identity, zvaná **phishing**. Mezi další „top-ten“ kybernetické zločiny řadíme internetové podvody, hacking, porušování AP, e-mailové hrozby, obtěžování a šíření dětské pornografie. Tyto delikty jsou nejčastěji páchány pomocí dvou běžných metod – sociálního inženýrství a malware, které ve své kombinaci mohou dosáhnout katastrofálních výsledků. U EIK vyvstává několik **problémů**, které znemožňují její odhalení. Zaprvé je to prostředí, ve kterém se odehrává. Kyberprostor je místem, kde neplatí žádná vynutitelná pravidla a kde jednotliví uživatelé mohou vystupovat pod různými identitami (nicky, čísla ICQ, e-maily, domény atd.), které podle definice osobních údajů v zákoně č. 101/2000 Sb., o ochraně osobních údajů [24], mohou být chráněnými údaji. Zadruhé, jde o samotnou právní postižitelnost prostředí. Jak uvádí SMEJKAL [25], tzv. „počítačové právo“ (computer law) či „informatické právo“ je průřezovou právní disciplínou, která se zabývá nejrůznějšími právními obory a odvětvími, spojenými jedním společným prvkem - počítačem, jeho obsahem (daty a programy) a

[24] Česko. *Zákon o ochraně osobních údajů* [online] [cit. 2005-09-07]
[25] SMEJKAL, V. *Informační a počítačová kriminalita v České republice*

jeho příslušenstvím. Toto odvětví se vytváří napříč klasickými právními disciplínami, protože zasahuje do veřejnoprávní i soukromoprávní sféry, do procesních norem, do teritoriálních i mezinárodních úprav, do občanského, obchodního, správního, trestního i dalších oblastí práva. V zahraničí se používá termín „cyber law“ (kybernetické právo), a to zejména ve spojení s právem na internetu.

4.9.8.1 Internet

Jen těžko bychom hledali odvětví, v němž by Internet nezačínal hrát důležitou roli. Společnosti, pro které byli dříve počítače jenom nástrojem, mění svou strategii. A je jedno, jestli jsou z bankovnictví nebo třeba z lehkého průmyslu či dokonce z metalurgického odvětví. Internet znamená skutečnou změnu, změnu srovnatelnou snad jen s průmyslovou revolucí. Světoví leadeři si uvědomují, že koláč se znovu přerozděluje. Nás pochopitelně nejvíce zajímá ryzí internetová kriminalita. Přes absenci průkazných policejních statistik nejčetnější odvětví, se kterými se tato skupina potýká.

Trestnou činnost spojenou s počítačovými sítěmi a zejména s Internetem můžeme klasifikovat do dvou základních kategorií:

1) zpřístupňování informací, které mohou někomu způsobit újmu nebo založit spáchání trestného činu nebo naopak shromažďování informací o osobách za účelem jejich pozdějšího nelegálního využití – nebo informační trestná činnosti

2) páchání trestné činnosti v internetovém prostředí, a to takové činnosti, kterou lze páchat díky vlastnostem Internetu – neboli internetová trestná činnost

Následující typy útoků v prostředí internetu dostávají zcela nový rozměr. Internet, resp. jeho služby (e-mail, diskusní fóra, blogy, instant messaging a webové stránky), umožňují anonymní vyjadřování a šíření různých názorů. Uživatelé internetu mohou páchat různé nezákonné aktivity pod falešnou identitou, díky níž padají veškeré zábrany, které by měli v reálném světě. Do této kategorie trestných činů bychom mohli zahrnout činnosti, které u nás zatím nejsou moc známy. Např. **cyberbullying** (kybernetická šikana), která spočívá v zasílání škodlivých či krutých textů, popř. obrázků prostřednictvím internetu. Podmnožinu těchto činů tvoří **cyberstalking** (obtěžování po internetu), u kterého jde o projev násilí – psychického teroru. Jsou rozeznávány dvě

formy cyberstalkingu: rozesílání výhružných e-mailů vyjadřující nenávist a obscénnosti a rozesílání e-mailů v podobě virů a spamu.

Zásadní problém spočívá v určení **odpovědnosti** za „závadný obsah“. V naší republice je odpovědnost poskytovatele služeb (providera) za obsah informací poskytovaných na internetu upravena v zákoně č. **480/2004 Sb.**, o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Dle tohoto zákona **není** provider odpovědný za obsah cizích webových stránek, kterým umožňuje umístění na svém serveru, a **nemá** tedy povinnost jejich obsah aktivně monitorovat. Pokud se však dozví o protiprávní povaze obsahu stránek (extremistické názory, dětská pornografie atd.), má povinnost dotčené stránky odstranit, respektive znepřístupnit. Provideři mají dále **povinnost** uchovávat údaje o připojení svých uživatelů, a to po dobu půl roku.

4.9.8.2 Zakázaná pornografie

Pornografický materiál patří na Internetu stále k nejvyhledávanějším. Anonymita, přitom efektivní komunikace a rychlý přenos dat prostřednictvím výměnných sítí nahrávají také jeho nelegální formě.

„Sice se nezvýšil počet osob, kteří takovou činnost páchají, ale razantně se zvýšil počet útoků, kdy uživatel rychle zaplaví nějakým materiálem celý svět. Lépe samozřejmě za podpory IT fungují i pedofilní či zoofilní komunity. Právě v našem prostředí Internetu se objevuje stále více domlouvání zakázaných sexuálních aktivit na dětech a se zvířaty. Pachatelé hledají své možnosti v oblasti chatů a diskusních skupin,“ Policii prý v boji proti nelegální pornografii hodně pomáhají oznámení obyčejných internetových uživatelů. Šíření pornografie v prostředí internetu je po warezu a hackingu další nejčastěji páchanou ilegální aktivitou. Provozovatelé pornografických serverů, kteří vyžadují registraci a poplatek pro přístup k pornografickým materiálům, tak vydělávají velké peníze. Existují pochopitelně i servery zpřístupňující pornografické materiály zdarma, ty ale své peníze vydělávají prostřednictvím zmiňovaného spyware apod. Vedle webových stránek jsou zdrojem, resp. distribučním kanálem **sítě P2P**. Tyto sítě jsou využívány také k obchodu s fotografiemi či videonahrávkami, k peněžním transakcím a k informacím týkající se dětské sexuální turistiky. Část distribuce dětské pornografie má komerční charakter a je spojena s mezinárodním organizovaným zločinem.

4.9.8.3 Extremistické projevy

Na druhém místě se podle očekávání objevil extremistický obsah, jemuž rovněž Internet a web poskytují živnou půdu. „Internet je takový, jaká je společnost. Podstatné je, aby určité aktivity nebyly za využití IT vydávány s nějakým masivním přesvědčovacím účinkem, který je založen na porušování práv jiných osob či skupin obyvatelstva.“ Policie nejčastěji zaznamenává sektářské, nacistické, neonacistické, trockistické, ultraradikálně komunistické, českofašistické, extrémně nacionalistické, antifašistické, ekoradikalistické a ekofašistické aktivity. **Extremismus** je chápán především jako projev nesnášenlivosti doprovázený agresivním jednáním vůči zjevně odlišným jedincům či skupinám. Hnutí a skupiny, které můžeme označit jako extremistické, podle DASTYCHA [26] prosazují **medializaci svých myšlenek** velmi těžce, a tak využívají internetu jakožto média „pro všechny“. Neexistuje zde regulace ani cenzura obsahu, každý si zde může říkat a šířit, co chce. Internet je využíván i ke **komunikaci** mezi jednotlivými národními organizacemi těchto skupin a také se jeho prostřednictvím **distribuují** CD s extremistickými hudebními nahrávkami. Na českém webu můžeme najít zejména weby popisující antisemitské názory a činnosti neonacistických skupin. Postižitelnost takovýchto skupin na internetu je velkým problémem. *„Celá oblast extremismu těží z toho, že v některých zemích není prezentace těchto názorů trestná a je brána jako svoboda projevu“*. [27]

Většina stránek je totiž registrována v USA, kde není extremismus považován za trestný čin. Policie je proto nucena spolupracovat se zahraničím.

4.9.8.4 Zneužití platebních a obchodních systémů

Zpočátku se jednalo o zneužívání platebních karet, dnes se objevují i podvržená obchodní místa a nastávají problémy s aukcemi.“

Připomeňme, že v zahraničí se rozmáhá phishing a objevil se pharming. Útoky jsou cíleny i na české uživatele, zatím ale převážně ze zahraničí, což jejich účinnost pochopitelně snižuje (jinak se pohybuje okolo pěti procent). Z pohledu poškozeného u nás zatím nebyl řešen žádný podobný případ, policie doposud řešila tyto kauzy pro cizí kriminalistické služby v rámci mezinárodní spolupráce. Je však jen otázkou času, kdy phishing využije k obohacení také vykutálený český „rybář“.

[26] DASTYCH, J. *Extremismus na Internetu* [online].11/2000 cit. 2006-03-16]
[27] SVATOŠOVÁ, H. *P2P sítě : přísné pojetí odpovědnosti podle Nejvyššího soudu USA zákon* [online] 5.7.2005

„Rovněž tak pharming není u nás příliš vyvinutou kriminalitou, i když lze počítat s jeho rozšířením vzhledem ke stále větší penetraci internetových obchodních služeb a se zdokonalujícím se sociálním inženýrstvím pachatelů."

4.9.8.5 Porušování autorského práva

Porušování autorského práva se většinou týká softwarového pirátství (viz výše), výjimkou rozhodně není ani na Internetu. Policii dělají vrásky na čele především výměnné sítě.

„Ty jsou obrovským problémem v souvislosti s porušováním autorských práv. Těží z globálnosti Internetu, nejasnosti kvůli právnímu určení, kde se skutek stal a kam patří jeho vyšetřování v rámci světa, a rovněž ve složitostech a zdlouhavosti zahraniční spolupráce s některými zeměmi. Porušování AP a práv souvisejících s právem autorským je především **občanskoprávní delikt**, podle okolností však může naplnit znaky skutkové podstaty trestného činu porušování AP, práv souvisejících s právem autorským a práv k databázi podle **§152 trestního zákona (dále jen Tr.Z.)** nebo přestupku na úseku kultury podle **§32 Zák. č. 200/1990 Sb. o přestupcích**. [28] Z výše uvedené definice AutZ vyplývá, že ochrana a potažmo pirátství se může týkat jak **SW** (rozmnoženiny nebo kopie bez souhlasu autorů jsou porušením AP, platí výluka volného užití), tak děl **hudebních** a **filmových** (zhotovování rozmnoženin těchto děl a záznamů lze jen s výslovným souhlasem nositelů práv uděleným licencí či smlouvou, pokud nejde o zhotovení jediné kopie pro osobní potřebu), **databází** (chráněny od 1.12.2000 a obdobně jako u SW nelze pořizovat rozmnoženiny bez souhlasu pořizovatele databáze, s ohledem na **§88** a **§30** odst. 1 Aut.Z. není možné zhotovit záložní kopii podstatné části databáze bez souhlasu jejího pořizovatele) i **webových stránek**. Internet a jeho služby se bezesporu stal stimulem pro **masové porušování AP**; na internetu padají veškeré bariéry. Zároveň je prostředím, které poskytuje nepřeberné množství různých pomůcek k překonání ochrany proti kopírování (generátory sériových čísel nebo tzv. cracky), návody pro hacking (zkušenosti nasdílené v rámci hackerské etiky) atd.

Problematika se týká zejména **majetkových práv** Aut. Z, a to práva dílo **užít** (§12), které rozeznává dále právo dílo **šířit** (§13) a **rozmnožovat** (§14), dále právo **volného užití** (§30), **ochrany** díla (§43-44) a počítačových programů (§65-66).

Pod pojmem **pirátství** chápeme neoprávněné nakládání s dílem, které je předmětem ochrany podle AP či práv souvisejících s právem autorským. Základní trestní

[28] *Česká protipirátská unie* [portál][cit. 2006-02-19]. Dostupný z WWW: <http://www.cpufilm.cz

odpovědnost za tuto činnost je dána **§152** TrZ - porušování autorských práv. LÁTAL[29] k tomu dodává, že při realizaci pirátství přichází v úvahu uplatnění i dalších ustanovení trestního zákona, a to **§150** TrZ (porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu) a **§149** TrZ (nekalá soutěž - vyrobený a distribuovaný plagiát parazituje na dobré pověsti oficiálního výrobce).

Softwarové pirátství je pravděpodobně nejproblematičtější oblastí neoprávněných zásahů do autorského díla. Každý uživatel počítače si shání SW dle svého zájmu, účelu a pochopitelně též finančních možností. Počítačovým programem nemáme na mysli jen různé kancelářské aplikace, rozmanité utility pro práci s grafikou, ale také hry, které jsou častou obětí softwarového pirátství u dětí a mládeže. Dalším oblíbeným artiklem, který se ocitá ve spárech pirátství, jsou **hudební** (nejčastěji v komprimovaném formátu MP3) a **filmová** díla (formát AVI, DivX apod.).

S pirátstvím je neodmyslitelně spjata problematika výroby a užívání tzv. **cracků** (§43 TrZ). Tímto pojmem rozumíme program, který umožňuje plně funkční užívání časově omezeného nebo jinak chráněného aplikačního programu nebo hry. Kromě cracků je na internetu také zveřejňováno velké množství sériových čísel (např. www.serials.com, www.serials.ws, www.t1000.net aj.) k nezměrnému počtu programů, po jejichž zadání se program stává plně funkčním. [30] Dalším typem překonávání důkladnější ochrany, a to tzv. hardwarového klíče, který je implementován u dražších programů, jako např. AutoCAD, se využívá tzv. **reverse ingeneering** (zpětná dekompilace systému).

Fenomén **warezu** je výsledkem nástupu moderních ICT, a to především internetu. Zatímco do nástupu warezu šlo o izolované obory pirátství v oblasti SW, hudby a videa, díky rychlé přenosové kapacitě internetu a stále se zdokonalujícím kompresním formátům dat spolu se zařízením pro jejich uchovávání, se dnes spojují všechny tyto tři činnosti do jedné. Princip warez scény je postaven na bázi **„non-profit“**. Drtivá většina lidí toto pravidlo respektuje a chová se podle něj. Jediné, co jednotlivec nebo skupina získají, je **respekt konkurenčních skupin** v případě kvalitních výsledků. Warez bývá doménou skupin, které se vyznačují poměrně vysokou mírou specializace a dělby práce. V každé takové skupině většinou bývá jeden či několik crackerů, kteří se zabývají obcházením ochrany proti kopírování zabudované v programech. Další se věnují propagaci, tvorbě webových stránek s upoutávkami na své „produkty“, tvorbou katalogů, které jsou rozesílány, reklamních letáků atp. [31] Nejpopulárnější formou pro sdílení nelegálního

[29] KŘÍŽ, L. *X-vize budoucí bezpečnosti* [online]. 1.1.2006
[30] Česko. Ministerstvo vnitra ČR. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení*
[31] LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*. 1998

obsahu jsou tzv. **peer-to-peer sítě - P2P** (opak architektury klient-server). Oblíbenost výměnných sítí spočívá v tom, že s rostoucím množstvím uživatelů celková dostupná přenosová kapacita roste, zatímco u modelu client-server, kdy se uživatelé musí dělit o konstantní kapacitu serveru, průměrná přenosová rychlost při nárůstu uživatelů klesá. Tyto programy pro sdílení souborů, jako např. *Direct Connect (DC, DC++), BitTorrent, WarezP2P* aj., umožňují vyhledávání podle jména, žánru či klíčového slova týkající se hudby, filmů či SW. Odhaduje se, že na internetu se nachází téměř miliarda nelegálně nasdílených hudebních skladeb. Dnešní anonymní výměnné sítě umožňují (legální i nelegální) výměnu souborů s prakticky nulovou mírou odpovědnosti jednotlivých uživatelů. Dochází však k žalobám (zejména v USA) na provozovatele takových sítí, které podávají zástupci autorů a organizace, jako je *RIAA* či *MPAA*. Jako příklad můžeme uvést rozhodnutí amerického Nejvyššího soudu, podle kterého byli provozovatelé sítí P2P služby *Grokster* a *StreamCast* zodpovědní za porušování AP jejich uživateli. RIAA ihned reagovala rozesláním dopisů sedmi dalším provozovatelům P2P sítí, ve kterých je nabádá k ukončení jejich činnosti. [32] Prezident RIAA *Cary Herman* přišel s novým označením pro ty, kteří si nelegálně stahují hudbu, a sice „songlifter“ (odvozeno z „shoplifter“, označení pro zloděje v obchodě).

Většina západních zemí posuzuje tvorbu a distribuci warez za nelegální činnost, země třetího světa ji naopak považují buď za zcela legální, nebo přinejmenším volně trpěnou až zcela ignorovanou. V naší republice je kopírování a šíření autorských děl bez povolení autora trestný čin podle **§152** Tr.Z. - porušování autorského práva, práv souvisejících s právem autorským a práv k databázi. **Použití** jiného autorského díla než programu či elektronické databáze pro **vlastní potřebu** (podle §30 Aut.Z.) je však v ČR legální i bez svolení autora. Tedy např. stažením filmu a jeho užitím pro vlastní potřebu není český zákon porušen, třebaže film či hudba jsou šířeny v rozporu se zákonem. Kompenzace autorům za užití pro osobní potřebu spočívá v paušálních platbách.

Porušování autorských práv se týká také samotných **webových stránek**, neboť jde o díla, která jsou výsledkem jedinečné tvůrčí činnosti autora a mohou být chráněna AutZ. Webové stránky mají dvě podoby, jednak samotný **zdrojový kód** (HTML, PHP atd.), jednak **cílovou podobu**, kterou uživatel vidí v prohlížeči (design i obsah). V mnoha lidech přetrvává chybné povědomí, že to, co je „na internetu“, je zadarmo a neplatí zde žádná legislativní omezení. Podle **§44** AutZ sem dále můžeme zahrnout **zásahy hackerů do webových stránek**, kdy dochází k pozměnění zdrojového kódu původní stránky (tzv. defacement).

[32] SMEJKAL, V. *Informační a počítačová kriminalita v České republice*

Další oblastí porušování autorských práv, kde může být páchána informační kriminalita, jsou **jména domén v internetu**. **Česká legislativa** nestanovuje žádná pravidla pro registraci doménového jména, přidělování funguje na základě systému "kdo dřív přijde". Doménové jméno je tak přiděleno prvnímu žadateli. Na existenci jiných práv se nebere ohled - rozhodující je okamžik přijetí žádosti. Subjekt, který žádost o doménu podá a je mu přidělena, k ní má vlastnická práva a povinnosti. Registrace probíhá podle podmínek zveřejněných na webových stranách www.nic.cz pomocí smlouvy o registraci doménového jména. Tato situace s sebou přináší řadu konfliktních situací - není totiž stanoven právní režim domény. [33] Vznikající spory o domény lze rozdělit na spory se **spekulanty** (doménu zaregistruje subjekt, který k ní nemá žádný vztah, v úmyslu ji později se ziskem prodat) a spory s **konkurenty** (spor se seriozním zájemcem o doménu, který má zájem registrovanou adresu využívat). Pod pojmem **Cybersquatting** či také **Domain Name Grabbing** rozumíme zaregistrování doménového jména shodného nebo zaměnitelného se známými ochrannými známkami či významnými firmami. Majitel nově získaných domén potom spekuluje s tím, že doménu s nemalým ziskem prodá majitelům ochranných známek či firem. Dnes již tato činnosti ustupuje do pozadí, neboť svůj „boom“ zažila v době, kdy firmy na internet teprve vstupovaly. Ale stále najde své opodstatnění např. při uvádění nového produktu na trh, kdy jsou **squatteři** rychlejší než výrobci produktu, kteří jsou pak nuceni od nich doménu odkoupit za nepřiměřeně vysoké částky. Dalšími formami doménového pirátství jsou [34] různá nekalá soutěžní jednání, kdy dochází např. k parazitování na pověsti, pokud si někdo založí stránku se jménem věhlasného produktu a provozuje na ní svůj internetový obchod apod.

4.9.8.6 Pomluvy a diskreditace osob

Karel Kuchařík, na Policii ČR (dále jen PČR) v oblasti IT nejpovolanější z povolaných, považuje pomluvy, výhružky a různé poplašné zprávy za zvláštní trend na českém Internetu. „Není narůstající, ale mění své prostředí – na tom je vidět, jak lidé v naší společnosti přecházejí na nové komunikační technologie. Někdy i s vírou, že si tím zajišťují naprostou anonymitu, což ve skutečnost naštěstí není pravda.“

Za pomluvu na webovém diskusním fóru už dokonce padl trest; tento příběh byl zveřejněn v článku Vězení za diskusi na webu!

[33] LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*. 1998.
[34] JUŘÍK, P. *Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet.* 1. vyd. Praha 2003. 312s. ISBN 80-7201-311-4

4.9.8.7 Skenování portů

Skenování portů (port scanning) je průzkumná technika, hojně využívaná přínosnými servery, ale také hackery jako příprava k útokům. Dodnes se vedou spory o tom, zda je skenování legální, nelegální nebo neslušné. Pokud nenastane následný útok, je obtížné prokazovat protizákonný úmysl. Cílová místa často o takovém chování ani neví, nebo mu nepřikládají potřebnou pozornost. Když už k nezákonné činnosti dojde, existuje tendence vše ututlat.

„V tomto případě nastává efekt zdi a snaha vlastního vyřešení, aby daný poškozený nebyl znevýhodněn ve vztahu k prezentaci vlastních bezpečnostních systémů. To se týká i takových subjektů, jako jsou některé banky. Policie se tím pádem o takovém jednání ani nedoví a nemá tedy co vyšetřovat. Přesto taková kriminalita existuje."

Na druhou stranu chápe postoj poškozených, kteří nemají k PČR důvěru. Ta se tím pádem ani nemůže na konkrétních případech zdokonalovat: „Je to tak trochu zamotaný kruh, z něhož těží především útočníci," a poukazuje na ochranu proti zveřejnění informací o poškozeném, která funguje ve Velké Británii.

Internet jako takový podle SMEJKALA [35] není subjektem práva – nemá právní subjektivitu, není ani ryze hmotným předmětem, ani čistě nehmotným statkem a dokonce není ani objektivní právní skutečností, nezávislou na lidském chování. Jde o informační a komunikační systém, který jako celek nemá svého majitele. **Subjekty** právních vztahů jsou v tomto případě uživatelé internetu, poskytovatelé služeb, vlastníci serverů a sítí apod. Právní vztahy při přenosu dat v internetu vznikají mezi jednotlivými provozovateli sítí, ale především mezi koncovými uživateli a providerem. **Objekty** práva jsou hmotné i nehmotné objekty, chování, resp. výsledky určitého chování apod. Z naznačených charakteristik internetu vyplývá jakási bezmocnost uchopit ho v rámci stávajícího právního řádu. Proto se na internet pohlíží jako na přenosové médium - umožňující využívání poskytovaných služeb.

Právní režim se řídí dvěma principy:

- prioritní **princip teritoriality**, který uplatňuje právo země, kde je služba poskytována (sídlo poskytovatele služeb, příp. umístění serveru)
- sekundární **princip práva upravující druh činnosti**, která je takto realizována, bez ohledu na médium (obchodní, občanský zákoník, autorský zákon apod.). Charakter

[35] SMEJKAL, V. *Informační a počítačová kriminalita v České republice*

internetového prostředí (globální, bez časových a prostorových hranic, anonymní aj.) však tuto situaci velmi komplikuje.

Vcelku zásadní problém, který nastává při **odhalovaní EIK**, představuje sběr důkazních prostředků, které by mohly sloužit k usvědčení pachatele. Digitální důkazy jsou totiž nehmotné a přechodné povahy. Situace je komplikována snahou pachatelů zahlazovat po sobě veškeré stopy, zejména v případě hackingu, využíváním anonymizérů [17] atd. Jako zdroje důkazních informací v kyberprostoru můžeme využít:

- **e-mailové adresy** a další informace umístěné v hlavičce zprávy - received (server umístí do hlavičky název a IP adresu počítače, od kterého zprávu přijal), **webových stránek** (obsah, doménové jméno), **serveru** (IP adresa) – záznamů providera (též lze zjistit uživatelské jméno, heslo aj. osobní údaje), **log soubory** – např. u služby přístupu k síti, u FTP, **diskusních skupin**, které využívají protokol NNTP [18] **přístupových čísel** – ze záznamů providera, ten je schopen podle IP adresy zjistit, na jaké telefonní číslo bylo voláno.

4.9.8.8 Útoky na data

Většinou jde o útoky využívající protokolu **TCP/IP** [19], který je starý přes 30 let a ne vše tedy dnes funguje optimálně. V době vývoje protokolu se nepředpokládalo, že počítačová síť bude celosvětově rozšířená. K vrstvám, které jsou **náchylné k útokům**, patří síťová, transportní a linková vrstva. Pachatel, který se snaží získat přístup k určitým internetovým serverům, se snaží postupovat tak, aby nemohl být zpětně identifikován. Při každém pokusu o přístup k jinému počítači se tento počítač dozví minimálně **IP adresu** [20] pachatelova počítače. Ta se vkládá při síťové komunikaci do každého paketu, aby webový server a router (směrovač) na internetu věděl, kam má vyřízený požadavek zaslat. Pokud uživatel nemá trvalé připojení k internetu, zpravidla dostává při každém připojení jinou IP adresu. **Pouze poskytovatel připojení** může na základě souborů se záznamovými protokoly zjistit, který uživatel, kdy a pod jakou IP adresou se připojil na internet. Z důvodu ochrany dat však tyto informace nesmí kromě orgánů činných v trestním řízení nikomu poskytnout. Záleží jen na správci serveru, jestli si dá práci s porovnáváním hledané IP adresy se seznamem neznámých, popř. anonymních vlastníků a jim přidělených IP adres. Pro větší zabezpečení anonymity používají hackeři jednu nebo více „přestupních stanic“. Jde o tzv. **aktivní proxy server** nebo VPN [21]. Odesílaná a přijímaná data se tak nejprve umístí do této přestupní stanice, která se následně postará o

jejich správné přesměrování. Server, na nějž se posílají požadavky, se tedy prakticky dozví pouze IP adresu přestupní stanice. [36]

Podle studie provedené specialisty z Washingtonské univerzity [22] obsahuje každá 67. webová stránka (reprezentativní statistický vzorek tvořil 18 milionů webových stránek) nějaký malware. Pod pojmem malware [23] rozumíme **škodlivý SW**, který je dále zneužíván k průnikům do systému a následnému zneužití či destrukci dat, případně celého systému. V současnosti jsou uživatelé internetu rozděleni na dva tábory: ti, kteří používají pokročilé zabezpečovací programy a ti, kteří prostřednictvím svých nechráněných počítačů škodlivý SW šíří dál. Mezi typický malware řadíme počítačové viry, červy, trojské koně, rootkity, keyloggery, spyware, hijackery, dialery apod. **Opatřeními** proti škodlivému SW jsou instalace a pravidelné aktualizace antivirových programů (např. *AVG*, *Avast!*, *Norton Antivirus* atd.), antispywarových programů (např. *SpywareBlaster*, *SpyBlocker*, *Spybot Search&destroy* atd.), programů na odstraňování rootkitu (např. *RootkitRevealer*, *BlackLight* atd.), používání osobního firewallu (např. *Zone Alarm*) a antidialerů (např. *MrSoft Antidialer*). K tomu můžeme dodat radu - nestahovat z internetu vše, co je k dispozici „zadarmo“ a brát v potaz důvěryhodnost serverů.

Podle statistik z roku 2004 přesáhl počet škodlivých kódů hranici 100 000, ale jde jen o orientační číslo (různé verze virů, jejich modifikace atd.). Viry se šíří především elektronickou poštou, např. v roce 2003 byl celosvětový poměr e-mailů a virů v nich 33:1, o rok později se počet zdvojnásobil na 16:1. [37] Škodlivé kódy se už nepíší jen pro zábavu nebo reputaci jejich autorů, ale hlavně k odcizení dat z napadených počítačů či k instalaci jiných zákeřných programů. Uvedený malware **využívá bezpečnostních nedostatků** systémů a umožňuje zneužívání počítačů k provádění dalších ilegálních činností (šíření dětské pornografie, rozesílání spamu, DDoS útoky, krádež identity atd.), které jsou popisovány v následujících kapitolách. Utěšující zprávou je, že se neustále **zkracuje doba** mezi zranitelností SW a objevením příčiny, která příslušnou chybu využívá. Podle statistik společnosti *X-Force* [38], která analyzuje nejnovější trendy v bezpečnosti a aktuálním ohrožení, dochází k časové kompresi - např. v roce 2002 odhalení viru *Slammer* trvalo 6 měsíců, v roce 2003 byl vir *Blaster* odhalen již za 26 dnů a v loňském roce stačily k odhalení viru *Zotob* pouhé dva dny.

---

28 POŽÁR, J. Některé trendy informační války, počítačové kriminality a kyberterorismu. In *Bezpečnost v podmínkách organizací a institucí ČR: sborník z mezinárodní konference, 20. května 2005, Praha* [online]. Praha: Soukromá VŠ ekonomických studií, 2005. ISBN 80-86744-49-3

[37] PŘIBYL, T. Hacker: *Klávesnice jako zbraň* : Rozhovor s nejslavnějším hackerem světa Kevinem Mitnickem. *PC World.* 2003

[38] HLAVENKA, J. *Phishing: Když si hacker podá ruku se zločincem*

Hackingem rozumíme neoprávněné získání přístupu k datům, tzv. průnik do systému jinou než standardní cestou. Po trestných činech vztahujících se k porušování AP jde o druhou nejčastější oblast EIK. Mezi těmito typy kriminality existuje ovšem podle MATĚJKY[39] propastný rozdíl. Zatímco u hackingu je patrná tendence ke zpřísňování postihu, masovost porušování AP vede spíše k úvahám na téma udržitelnosti současné právní úpravy, neboť se jedná o čin, který v menší či větší míře páchá značná část počítačově gramotného obyvatelstva. Tyto trestné činy jsou páchány nepřímo, přes více internetových serverů, aby se snížila možnost identifikace skutečného umístění pachatelova počítače. Podmínkou průniku je síťová komunikace a též využívání různých bezpečnostních děr v systémech. Na internetu se nachází celá řada podpůrných programů i s popsanými postupy, jak průnik nejefektivněji spáchat. Hacking je lákavou činností počítačových nadšenců bez destruktivních záměrů, ale zároveň i vykalkulovanou aktivitou s cílem obohacení a poškození. Amatérské průniky do systémů lze většinou snadno odhalit, zatímco v závažných případech mnohdy zůstává pachatel neodhalen. [40]

Technika, která je při počítačovém útoku hojně aplikována, se nazývá **sociální inženýrství** (social engineering), tzv. sociotechnika. Sociální inženýrství využívá nátlakové metody v podobě časového limitu či hrozícího nebezpečí. Další záminkou k získání důvěry uživatelů je fakt, že např. u e-mailu je odesílatelem subjekt s vyšší autoritou, obsah slibuje nevídané slevy či nabízí něco zdarma atd. Průkopníkem této metody je **Kevin Mitnick**, který se touto tématikou zabývá ve dvou vydaných publikacích (*Umění klamu* a *Umění průniku*). Jde o velmi nebezpečnou techniku, a to nejen počítačového útoku, neboť je zaměřena na **nejslabší článek** celého systému, kterým bývá člověk. Jakmile selže lidský faktor, jsou veškerá implementovaná bezpečnostní opatření zbytečná. [41]

Pod pojmem **phreaking** [24] rozumíme činnost, která vede k bezplatnému využívání telefonních linek (napichování služby, hovory na účet někoho jiného nebo telekomunikační firmy). Phreaking má bohatou čtyřicetiletou historii. Původní telefandové pokládali phreaking za jistou formu zábavy. Postupně však phreaking přestal být módou a **phreakeři** (používají ukradené telekomunikační informace pro přístup k dalším počítačům) či **phrackeři** [25] (snaží se napadat programy a zneužívat databáze telefonních společností za účelem získání telefonních služeb zdarma) se začali učit

[39] LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista.* 1998, č. 3, s. 3-15

[40] Česko. Ministerstvo vnitra ČR. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení*

[41] PROSISE, Ch; MANDIA, K. *Počítačový útok : detekce, obrana a okamžitá náprava.* Praha : Computer Press, 2002. 432 s. ISBN 80-7226-682-9

pronikat do počítačových systémů. Hackeři (white hats) se od této skupiny distancují. Díky digitalizaci telefonů je phreaking na značném ústupu – na rozdíl od rozmáhajícího se phishingu.

Phishing [26] a **pharming** [27] jsou zřejmě nejnebezpečnější formou využití spamu či jiných útoků, která dnes existuje. Phishing (také znám pod pojmy „brand spoofing“ a „carding“) historicky navazuje na aktivity phrackerů, těžiště jejich zájmu nejsou čísla telefonních karet, ale krádež obecnějších **privátních citlivých informací** týkajících se jedince. Těmito údaji mohou být především údaje o platební kartě nebo krádež přístupového jména a hesla k různým internetovým službám, s jejichž pomocí lze na dálku manipulovat s bankovním kontem. [42] Tyto nelegálně získané údaje jsou pak zneužity např. při převodu peněz, internetových nákupech, aukcích a jiných internetových podvodech. Phishing je běžnou metodou **krádeže identity**. Nejčastěji je prováděn pomocí naprosto legitimně a oficiálně vypadajících e-mailů, které obsahují formulář čekající na uživatelovo vyplnění a odeslání. Na phishing navazuje sofistikovanější metoda - **pharming**, která je sice známa už několik let, ale svůj rozvoj zažívá až v poslední době. Hlavní metodou phishingu a pharmingu je **sociální inženýrství** [28], které je doplněno dalšími prvky zvyšující důvěryhodnost, např. zfalšovaná e-mailová adresa, napodobená grafika, znalost terminologie atd. **Principem phishingu** je vyplnění formuláře, který žádá o potvrzení nebo doplnění např. bankovních údajů, jako jsou čísla kreditních karet, PIN apod., přímo v e-mailu. **Pharming** je mnohem větším nebezpečím, které je obtížně rozpoznatelné. Tajemství spočívá v překládání URL adresy do formátu IP adresy prostřednictvím DNS serverů. Útočníci se pokoušejí najít špatně zabezpečený server, v němž následně přepíší IP adresu určenou např. pro URL banky IP adresou falešné stránky. Po **odeslání** požadovaných dat nastává „chycení do sítě“. Obětí phishingu a pharmingu jsou jednak důvěřiví uživatelé, kteří se stanou cílem, a jednak instituce, u kterých měli uživatelé účet. Ty musí investovat značné prostředky a zdroje do různých reklamací a šetření. Dalším dopadem je pokles důvěryhodnosti takových institucí a možný odliv zákazníků ke konkurenci či obava zákazníků z využívání služeb elektronického bankovnictví.

Opatřením proti phishingu je věnována značná pozornost (např. prezident Bush zařadil boj proti phishingu do svého volebního programu). V roce 2004 oznámili zástupci řady podniků a donucovacích orgánů založení skupiny *Digital PhishNet*, která se zaměřuje na pomoc a podporu při dopadení a stíhání osob, které jsou zodpovědné za

[42] FOLTZ, B C. Cyberterrorism, computer crime and reality. *Information Management & Computer Security*. 2004

spáchání trestných činů proti zákazníkům prostřednictvím phishingu. Dále byla založena organizace *Anti-Phishing Working Group*. Pro to, abychom nenalétli na phishigový e-mail, můžeme udělat pár maličkostí. První efektivní ochranou je zásada neklikat na odkaz, který je v e-mailu uveden, ale zadávat adresu instituce přímo do adresového řádku prohlížeče. Případně můžeme e-mail v HTML formátu otevřít přímo v internetovém prohlížeči. Pohybem kurzoru myši nad odkazem se pak ve stavovém řádku objeví odkaz, na který bude stránka přesměrována. S narůstajícím výskytem případů phishingu vytasily své zbraně i softwarové firmy. Zabezpečení slibuje např. nástroj *Netcraft Toolbar*, který kontroluje u příslušného registru domén původ (geografické umístění) a aktuálnost domény, která se vyskytuje v odkazu e-mailu. Po krátké analýze vizuálně zobrazí důvěryhodnost stránky. Další podobně zaměřenou utilitou je *EarthLink Toolbar*.

Pharming na rozdíl od phishingu využívá technologii zvanou **DNS cache-poisoning** – otrávení paměti DNS záznamů. Principem pharmingu je modifikace záznamů v lokální paměti IP adres, tzn. místo korektní IP adresy je záznam změněn na podvrženou adresu. Když se pak uživatel pokusí připojit k nějaké stránce, prohlížeč vezme modifikovaný záznam z paměti a na internetu vyhledá příslušný podvržený server. Uživatel tuto změnu vůbec nezaregistruje, neboť z jeho pohledu došlo ke zcela korektní operaci: zadal správný název instituce a stránka se korektně zobrazila. [43] Takto zmodifikované webové stránky, které z uživatelů lákají citlivé údaje, jsou velmi těžko odhalitelné, neboť neexistují déle než 48 hodin.

DoS útok (Denial of Service - odmítnutí služby) je typem útoku, který je namířen proti serveru, resp. celé síti připojené k internetu s cílem ochromit jejich provoz. Jde o útoky, při nichž je z mnoha míst vysláno velké množství požadavků na jeden server, který se pod jejich náporem zhroutí. Někdy je DoS útok použit jen jako pomocná akce k zahlazení stop, restartování vzdáleného počítače apod. **DDoS útok** (Distributed Denial of Service) jsou variantou DoS útoku, který je však prováděn souběžně z velkého množství počítačů. S pomocí tisíců počítačů na celém světě, které se nakazily škodlivým kódem a vytvořily tak **botnet**, je možno zahltit podnikové servery tisíci elektronických zpráv, čímž se zablokují veškeré skutečné transakce a komunikace serveru.

Pachatelé poté zašlou společnosti e-mail, ve kterém požadují finanční obnos pod hrozbou opakovaného útoku. Tento typ vydírání zaznamenal rozkvět zejména v posledních třech letech, kdy roste počet sítí, které zločinci mohou vzdáleně řídit a ovládat. V roce 2004 bylo zaznamenáno, že denně se z 30 000 počítačů stávají aktivní botnety, které jsou dokonce za vysoké finanční obnosy pronajímány. Uvedené technologie podle

[43] PŘIBYL, T. Informační bezpečnost v roce 2004. *PC World Security.* 2005, č. 1, s. 2-7

studie *McAfee* [44] nejvíce využívají zločinecké gangy z východní Evropy k poškozování webových serverů různých organizací a obchodních společností. Ač spouštění zmíněných útoků nevyžaduje žádné speciální znalosti – stačí stažení a spuštění speciálního SW -, **opatření** proti těmto útokům je poměrně složité (nastavování routerů, firewallů apod.).

4.9.8.9 Kybernetický terorismus a válka

Kybernetický terorismus (**kyberterorismus**)[45] je pojem, který zastřešuje kombinaci výše zmíněných útoků, které jsou **nasměrovány proti osobám či majetku** za účelem vyvolání strachu, vydírání nebo vymáhání ústupků. Dle **americké vlády** [29] je kyberterorismus vymezen jako prokalkulovaný, politicky motivovaný útok proti informačním a počítačovým systémům, počítačovým programům a datům, vedený subnárodními skupinami nebo tajnými agenty, jehož výsledkem je násilí proti nezúčastněným a nebojujícím osobám. V literatuře je uváděno mnoho definic kyberterorismu, od velmi širokého pojetí až po úzké vymezení pojmu. Na tento jev je pohlíženo ze dvou úhlů. Mnoho autorů[46] zastává **užší pojetí**, které kyberterorismus nepovažuje za hrozbu, a tvrdí, že se nikdy neobjevil a nemůže nikoho poškodit. Druhé, **širší pojetí** předpokládá, že kyberterorismus je skutečnou bezpečnostní hrozbou vlád a organizací na celém světě. Zdá se, že kyberterorismus se stává realitou - čím dál více jsme závislí na IS a ICT a jejich ohrožení - v podobě narůstajících kybernetických útoků - má za následek nedozírné škody a ztráty.

ICT představují pro vyspělé státy obrovskou **konkurenční výhodu**, zároveň však představují jejich **nejzranitelnější místo**. Útoky jsou často zaměřené proti vládním a jiným institucím a pro podporu politických, sociálních a ekonomických cílů. V ohrožení jsou banky, letiště, armádní řídící systémy, nemocnice a jiné instituce, které jsou závislé na počítačových sítích a databázích. ICT jsou zde využívány jako **nástroj** útoku pro manipulaci a zneužití cizích informačních systémů, ke krádeži nebo změně dat, příp. k přetížení a zahlcení IS. [47] ICT jsou však zároveň také **cílem** útoku, který je zaměřen na zničení IS a systémů, které jsou na něm závislé. Útoky na IS jsou pro teroristy z hlediska nákladů a potřebného vybavení velmi **efektivní**. S minimálními náklady mohou napáchat nevyčíslitelné škody, způsobit kolaps finančních, dopravních, mocenských či jiných

[44] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. 97 s. ISBN 80-7226-419-2
[45] FOLTZ, Bryan C. Cyberterrorism, computer crime and reality. *Information Management & Computer Security*. 2004, vol. 12, no. 2, s. 154-166
[46] FOLTZ, B C. Cyberterrorism, computer crime and reality. *Information Management & Computer Security*. 2004, vol. 12, no. 2, s. 154-166
[47] PORADA, V. Kriminalita v digitálním prostředí a trendy aktuálních hrozeb. *Karlovarská právní revue.* 2005, č. 3, s.12-29

struktur a v nejhorším případě i ztráty životů. Klasickým **nástrojem** využívaným ke kyberteroristickým útokům jsou všechny zmíněné hrozby jako viry, DoS a DDoS útoky, spyware či backdoors aj., které mohou poškodit, zničit nebo měnit data, případně vyřadit systémy z provozu. Naznačené aktivity jsou pro společnost vždy velkým nebezpečím. Některé státy, bez ohledu na motivaci pachatelů, pokládají **jakýkoliv útok** na IS za kyberterorismus.

V souvislosti s kyberterorismem je třeba zmínit další jev, kterým je **kybernetická válka** (cyber war) či také **informační válka** (information war). Vzhledem k tomu, že ICT jsou ve vyspělých státech a ekonomikách integrovány do všech oblastí našeho života, není výjimkou ani armáda. Země na celém světě vyvíjejí a zavádějí kybernetické strategie s cílem zasáhnout velitelské a řídící struktury nepřítele, jeho logistiku, dopravu, systémy včasné výstrahy a další rozhodující vojenské funkce. Informační struktury jsou natolik důležité, že útok proti nim je považován za ekvivalent strategického úderu. **Klíčovým cílem** je dosáhnout informační převahy v prostoru kybernetického bojiště. Z literatury je známo několik úrovní kybernetické války (doplněk, omezená, neomezená). Nakonec se ukazuje, že v informační válce je nejzranitelnější ten, kdo je nejlépe připraven ji vést.

4.9.8.10 Elektronická pošta

Elektronická pošta je zneužívána k zasílání různých falešných varování **(hoaxes)** či prapodivných historek **(urban legends)**, které mají za úkol vyvolat ve čtenáři **paniku** či **zasáhnout jeho emoce**. Většinou se jedná o neškodná poselství. Mezi nejčastější patří varování o nových, avšak neexistujících virech **(virus hoaxes)** a srdceryvné příběhy o záchraně lidského života. Dá se říci, že tyto zprávy škodí pouze nepřímo, zahlcují však e-mailové schránky, okrádají uživatele o čas a hlavně ho přivádějí do světa lží. Jediné, co může uživatel před rozhodnutím, zda e-mail přepošle, či smaže, udělat, je **ověřit** si zprávu na speciálních serverech, shromažďujících veškeré hoaxy a městské legendy, které obíhají internetem (např. www.hoax.com, www.hoaxbuster.ciac.org, www.hoax.cz, www.snopes.com). Hoax se šíří vlastně pouze pomocí uživatelů, kteří ho v rámci solidarity rozesílají dalším a dalším uživatelům. *„Zlí jazykové tvrdí, že hoax je vlastně vir, který napadá tu část, která se nachází mezi židlí a klávesnicí“*. Přeposíláním e-mailů dochází ke zveřejňování velkého množství adres, které mohou být **zneužity** spammery.

Spam [30], čili nevyžádaná pošta často s komerčním propagačním obsahem, se stává každodenní přítěží uživatele elektronické pošty. Zřejmě první spam napsal zaměstnanec *Digital Equipment Corporation* v roce 1978 na adresy tehdejší sítě ARPANET. Dalším

spamem byla zpráva (s předmětem *make.money.fast!!*) rozeslána do diskusních skupin sítě USENET. **Cílové e-mailové adresy**, které zneužívají specializované direct marketingové firmy, jsou získávány většinou **automatickým prohledáváním** různých diskusních fór, konferencí nebo webových stránek. Mezi další zdroje adres patří **registrace** různorodých služeb, které jsou poskytovány „zdarma“ či posbírané adresy z hoaxů. Takto vytvořené databáze e-mailových adres jsou vysoce ceněným obchodním artiklem. Spammeři většinou zneužívají pro rozesílání e-mailů cizí SMTP servery, aby se tak vyhnuli umístění na tzv. black list spammerů a následně nebyli blokováni. **Poměr** doručeného spamu a korektních e-mailů rapidně stoupá. V roce 2003 bylo zjištěno, že 30 % všech odeslaných e-mailů tvořila nevyžádaná reklama, v roce 2004 již šlo o 60 %. Podle studie společnosti *Commtouch* [31] pochází **99 % celosvětového objemu spamu** pouze z pěti zemí (USA – 62 %, Čína, Jižní Korea, Rusko a Brazílie). V **Evropské unii** drží prvenství Rakousko.[48] Stoprocentně účinné **opatření** proti spamům v současnosti v podstatě neexistuje. Nabízí se však několik přístupů, které mohou problémy v dané oblasti alespoň zmírnit. Uživatel sám může filtrovat poštu, blokovat spamovské zdroje (některé freemailové služby umožňují blokaci všech podezřelých e-mailů i podle domény), instalovat antispamové programy (*Anti-Spam Enterprise Solution, GFI MailEssentials, JunkSweep* pro Outlook atd.) či skrýt svou adresu.

Kromě již zmíněného phishingu a pharmingu jsou na internetu provozovány různé podvodné aktivity, které nevyžadují příliš sofistikované technologie. Většinou jde o **finanční podvody**, kdy se důvěřivé oběti nechají nalákat na slíbené enormní zisky (obchodování s cennými papíry, různými komoditami atd.). Jde o podvody typu **letadla či pyramidy**. Podle FBI se 46 % internetových podvodů odehrává na **aukčních** stránkách (např. eBay). Uživatelé si v domnění seriózní koupě objednají zboží, zaplatí, leč z důvodu falešné identity se produktu už nedočkají. Na vzestupu jsou dle studie *McAfee* [49] **investiční a akciové** podvody. Ty spočívají v nákupu akcií relativně neznámých společností, o kterých jsou následně rozšířeny zfalšované obchodní informace. To má za následek nadhodnocení a navýšení ceny akcií, které jsou následně se ziskem prodány. Sítě investičních internetových podvodníků mají základny po celém světě a burzy vydávají černé listiny provozovatelů těchto podvodů. K dalším podvodům ve finanční oblasti dochází prostřednictvím falešně získaných identit využívaných k získání **kreditních karet**, které se staly standardem při placení po internetu. Na rozdíl od používání karet při

[48] McAfee. *Zpráva společnosti McAfee o virtuální kriminalitě: první celoevropská studie o organizovaném zločinu a internetu*
[49] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. 97 s. ISBN 80-7226-419-2

klasickém nakupování zde stačí zadat číslo kreditní karty a datum expirace, žádné další ověření není nutné. Základním bezpečnostním prvkem při placení po internetu je **zabezpečená komunikace** mezi počítačem zákazníka a počítačem - serverem internetového obchodníka.

Na závěr je vhodné uvést shrnutí **bezpečnostních a organizačních opatření**, kterých by se uživatelé ICT měli držet, aby nepřišli ani o data a informace, ani o finanční částky. Jde o jakousi obecnou prevenci proti nebezpečí internetu, která spočívá v následujících radách (dle anglické kampaně *Get Safe Online* [32]):

- instalace a aktualizace antivirového, antispywarového apod. SW
- instalace osobního firewallu
- zálohování
- instalace oprav (záplat) OS a aplikací
- používání prostého textu místo HTML e-mailů
- mazání spustitelných příloh
- používání důmyslných hesel
- šifrování elektronické komunikace (používání elektronického podpisu, PGP [33] atd.)
- ignorace spamu a odkazů typu *„Unscribe“* - ohlášení urážlivých, obtěžujících nebo podvodných e-mailů ISP a společnosti, jejíž jméno bylo zneužito

4.9.8.11 Rady pro online transakce

- neprozrazovat hesla, PIN apod.
- nevyplňovat e-mailové formuláře
- neklikat na odkazy v e-mailech
- hledat na stavovém řádku prohlížeče symbol zámku
- pravidelně kontrolovat bankovní účty a hlásit cokoliv podezřelého

Ministerstvo informatiky ČR oznámilo spuštění nového portálu *Bezpečně online* , který je inspirován výše uvedeným anglickým projektem (spíše jde tedy o kopii a překlad portálu). Web je zaměřen na počítačovou bezpečnost ve třech oblastech: *Chraňte svůj počítač* (viry, zálohy, antivirové programy atd.), *Chraňte sebe* (e-bankovnictví, e-nakupování, nebezpečný obsah atd.) a *Chraňte svoji firmu* (osobní údaje, šifrování, IBP atd.).

4.9.8.12 Srovnání českého a zahraničního prostředí

Česká republika se musí vypořádávat se stejnými problémy EIK jako ostatní země světa. Můžeme říci, že patříme k zemím s průměrným stavem kybernetických trestných činů. Rozdílné jsou možnosti represivních a preventivních složek, které se odvíjejí od vyspělosti ICT, zkušeností a možné spolupráce. Ve vyspělých zemích vznikají speciální týmy pro boj s kyberzločinem, většinou na centrální úrovni, popř. na vyšší úrovni jednotlivých územích celků. V naší republice se o potírání EIK stará Oddělení informační kriminality, které má ještě hodně před sebou. Obecně můžeme říci, že v naší **legislativě** neexistuje konkrétní zákon vztahující se k EIK, jednotlivé problémy jsou roztroušeny v různých právních předpisech, a to ne vždy zcela ideálně. V některých případech se s trestnými činy páchanými elektronicky vůbec nepočítá či nejsou dostatečně definovány jejich skutkové podstaty.

Podle zjištěných informací [50] dochází v ČR k oslabení počtu útoků po internetu a k poklesu zájmu pachatelů o medializaci. Zároveň stoupá nebezpečnost útoků a přibývá pachatelů, zneužívajících svých znalostí za úplatu. V oblasti **softwarového pirátství** z poslední globální studie [34], kterou vypracovala analytická společnost IDC [35] pro BSA, vyplývá:

- 41 % pirátského software (rok 2003 - 40 %) – svět 35 %
- ztráta 132 miliónů amerických dolarů – svět 33 miliard amerických dolarů
- za posledních deset let se míra nelegálního SW snížila o 20 %
- země s **nejvyšší mírou** softwarového pirátství (okolo 90 %): Vietnam, Čína, Ukrajina, Indonésie a Rusko
- země s **nejnižší mírou** softwarového pirátství (okolo 20 %): Singapur, USA, Nový Zéland, Dánsko, Lucembursko, Finsko a Švédsko
- Tímto výsledkem tak ČR[51] neobhájila svůj úspěch, kdy se jako jediná východoevropská země prosadila mezi dvacet nejlépe hodnocených zemí světa. Její

[50] Česko. Ministerstvo vnitra ČR. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení* [online][cit. 2005-23-07]
[51] PAUKERTOVÁ, V: *Elektronická informační kriminalita.*Praha,2006.114 s. Diplomová práce. Univerzita Karlova v Praze

místo zaujalo Portugalsko poté, co snížilo svou míru softwarového pirátství o jeden procentní bod na 40 %

Podle studie by **snížení** míry softwarového pirátství o 10 % do roku 2009 způsobilo:

- růst tuzemského IT sektoru z 47 na 58 %
- vznik 2 900 nových placených pracovních míst v oblasti IT
- přírůstek k domácímu HDP ve výši 951,9 milionu dolarů
- dalších 96,2 milionu dolarů ve formě daňových odvodů

Nejvíce případů softwarového pirátství je evidováno v Praze, severních Čechách a na jižní Moravě. Z hlediska výše způsobených škod se na první pozici umístily východní Čechy (téměř 11 milionů korun).Virus, jehož prostřednictvím se neznámý pachatel dostal k informacím o majitelích 40 miliónů kreditních karet v USA, ohrozil v ČR pouze lidi, kteří si ve Spojených státech zdržovali mezi srpnem 2004 a květnem 2005, nebo platili kartou na dálku, potvrdil bezpečnostní expert Sdružení pro bankovní karty Tomáš Janouch. „ V současné době se to může týkat stovek potencionálně ohrožených karet. Zatím není známo, že by vznikla nějaká škoda, „ uvedl. Počet ohrožených karet se však stále zvyšuje. ČSOB obdržela z USA 400 čísel ohrožených karet, které patří jejím klientům. Z ostatních bankovních domů nejvíce karet zablokovala GE Money (216). Česká spořitelna vymění zhruba 30 karet, zástupci Komerční banky hovoří o desítkách.

Odpověď na to, jak se také dají získat data z magnetických proužků platebních karet a jak „ vysoce ekonomicky zajímavá“ tato činnost je, dává článek z elektronického Magazínu Cardmag č. 04/2007(viz www.cardmag.cz/archiv/cm4_2007.pdf
Poslední zjištěné případy skimmmování dat na bankomatech v ČR v roce 2007 byly prováděny zejména tím způsobem, že pachatelé, převážně rumunské, moldavské či bulharské národnosti připevnili na vstupní štěrbinu pro platební kartu nástavce zakrývající, jak štěrbina pro kartu, tak i na výdej stvrzenek, nebo překryli celý prostor vpravo od obrazovky bankomatu, kde je štěrbina pro kartu, falešnou deskou napodobující originál nebo do prostoru u vstupní štěrbiny vlepili malý díl obsahující rovněž snímač magnetického proužku s elektronickou na záznam dat a baterií.

Dále na spodní desku bankomatu opět pomocí oboustranně lepící pásky nalepili falešnou desku s falešnou klávesnicí a elektronickou čtečkou k snímání kódu PIN dle stlačitelných tlačítek. Zařízení je vyrobené dosti kvalitně, pachatelé je ponechávají na

bankomatu v řádu hodin až dnů a pak zařízení sundají a na bezpečném místě stáhnou data do počítače na vyrobené platební karty vybírají peníze.

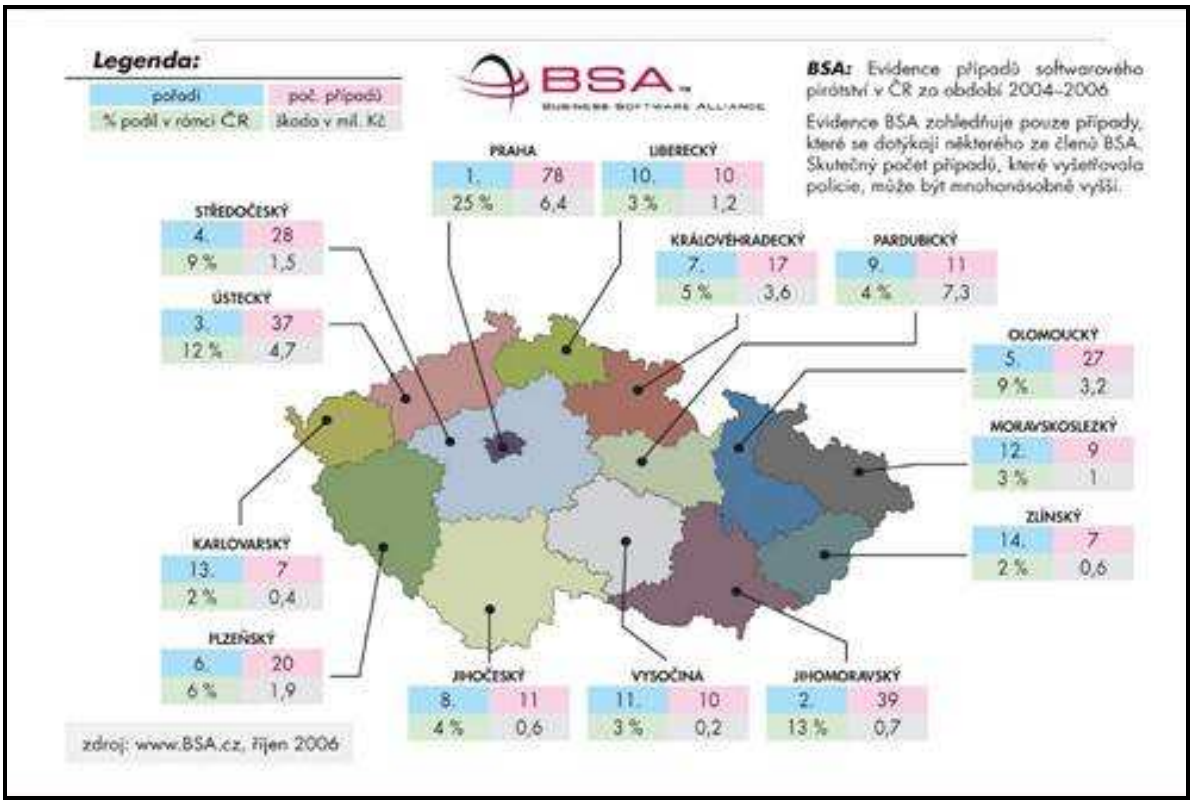
Variantou k výše uvedenému způsobu získávání kódu PIN pomocí celé falešné spodní desky bankomatu s falešnou klávesnicí jsou různé způsoby používání mobilních telefonů s fotoaparátem, resp. jejich částí. V tomto případě je opět mobil ukryt pod falešným krytem připevněných na klávesnici nebo z boku bankomatu. Při použití tohoto způsobu jsou data ukládána do mobilu, nebo mohou být pomocí Bluetooth přenášeny do jiného mobilu umístěného např. ve vozidle pachatelů vzdáleném až 100 metrů daleko nebo je možno tyto data odesílat pomocí SMS či MMS prakticky kamkoliv na světě.

Dalším způsobem, jak pachatelé získávají data z platebních karet v současné době v Evropě, je výměna originálního pokladního terminálu v hotelu, čerpací stanicí nebo velkoobchodě za upravený s tím, že po určitě době je upravený terminál rovněž odcizen. Výměna a zpět vzetí upraveného terminálu[52] je prováděna např. vloupáním, nebo za pomoci osoby zaměstnané v objektu nebo pomocí falešných servisních techniků na terminály apod. Následně jsou opět vyrobeny kopie platebních karet a používány k výběru peněz v bankomatech.
Tyto způsoby se zatím v České republice nevyskytly.

USA jsou asi nejprogresivnější zemí v oblasti používání ICT a tedy i patřičných zákonů a institucí. Situace je zde komplikována koexistencí federálních a státních zákonů, přičemž „počítačové právo“ je upravováno jak v trestněprávní, tak veřejnoprávní i soukromoprávní oblasti. *U.S. Copyright Law* upravuje ochranu duševního vlastnictví – rozdílem oproti našemu systému úpravy autorských děl je registrační princip, kdy podmínkou pro požívání ochrany je nutnost jeho přihlášení (U.S. Copyright Office). Ochrana SW jako literárního díla je ustanovena v *Computer Software Copyright Act*.

Základní rámec americké právní úpravy EIK tvoří dva americké zákony *Digital Millenium Copyright Act* (DCMA), který upřesňuje podmínky AP především ve vztahu k internetu, a *Communication Decency Act* (CDA), který představuje část federálního telekomunikačního zákona upravujícího omezení pro obsah elektronické komunikace.

[52] HRADECKÝ, M. *Platební prostředky jejich ochrana a padělání.*Praha 2008.ISBN 80-7312-055-0



Obrázek 2 - Konkrétní počet případů a způsobené škody v jednotlivých regionech [zdroj] 83.

Přijetí těchto zákonů předcházela dvě odlišná soudní rozhodnutí, která se týkala pomluvy prostřednictvím diskusního fóra. Americké orgány přijímají výklad **teritoriality práva** v souvislosti s internetem – podle některých soudních rozhodnutí je subjektem práva (i trestního stíhání) kdokoliv, kdo publikuje na internetu obsah, k němuž mohou mít přístup občané USA. K odhalování EIK slouží mnoho **center a agentur** jako *FBI, National Infrastructure Protection Center, National White Collar Crime Center, Internet Fraud Complaint Center, Computer Crime and Intellectual Property Section of DoJ* [36] (provozuje webové stránky www.cybercrime.gov, kde lze nalézt veškeré aktuální informace týkající se kybernetického zločinu – aktuality, legislativa, proběhlé kauzy, tiskové zprávy atd.), *Computer Hacking and Intellectual Property Unit of DoJ* atd. Na úrovni každého amerického státu je vytvořeno několik speciálních center či jednotek policie typu Computer Crimes Unit, Hi-Tech Crime Unit/Squad, Computer Crimes Task Force apod. Vláda USA vydala 60stránkový dokument *National Strategy to Secure Cyberspace* [37], který shrnuje strategické cíle zahrnující opatření proti kybernetickým útokům, snížení národní zranitelnosti a minimalizace škod způsobených kybernetickým zločinem. Zásadní priority tvoří rozvoj národního bezpečnostního systému v

kyberprostoru (program snížení kybernetických hrozeb, školící program, bezpečnost kyberprostoru na všech úrovních atd.)

Důvěra klientů v bezpečnost *platebních karet byla ve světovém tisku široce diskutována po té, co v polovině června 2005 došlo v USA ve zpracovatelském středisku ke kompromitování asi 40 miliónů čísel karet. Tiskové zprávy přinesly informace o rozsahu události a kompromitování databáze karet hackery nejdříve sváděly na počítačový vir.*

Ke jménům a číslům účtů až 40 miliónů vlastníků kreditních karet v USA se mohla prostřednictvím počítačového viru dostat nepovolaná osoba. Společnosti MasterCard International sdělila, že zřejmě dosud největší útok na finanční data se pravděpodobně dotkne všech amerických vydavatelů kreditních karet, Narušení bezpečnosti karet mělo původ u atlantského zpracovatele plateb pro banky a obchodníky CardSystoms Solutions. K průniku byl použit speciální virus, který vyhledává data o spotřebitelích s cílem podvodně vybrat peníze. Narušitel nemohl zjistit adresy ani čísla důchodového sociálního pojištění, takže nemohlo dojít ke zneužití cizí identity. Mohl se ale dostat ke jménům, bankám a číslům účtů, a využít je ke krádeži peněz z účtu karet. Z celkového počtu ohrožených účtů patří MasterCard 13,9 miliónu, avšak jen asi 68 000 z toho je vystaveno vysokému riziku. Celý případ vyšetřuje FBI. I když se tato událost zdá svým rozsahem enormní, škody nebudou velké. Lze odhadnout, že nějakým podvodem bývá postiženo 0,2% majitelů karet. Kromě možné ztráty důvěry v tento platební instrument konkrétním klientem to znamená, že konkrétní majitel karty bude podveden jednou za 500 let. I když se platebními kartami platí stále více na internetu, není zde riziko zneužití největší. Největším rizikem zůstává ztráta vlastní karty, pokud je před zablokováním používána k podvodným platbám. Vzhledem k tomu, že bývá vyšetřeno méně než 5% případů, okradeným držitelům kreditních karet může trvat léta, než si opět obnoví úvěruschopnost (míněno v úvěrových registrech). CardSystems Solutions je jedna z více než 100 firem v USA, které zpracovávají transakce. Oproti příslušným regulacím, vztahujícím se na kreditní společnosti, tato firma uchovává citlivá data o zákaznících na svém systému zakódována, místo aby je po jejich zpracování zničila. Tak se mohli hackeři dostat k číslům karet a třímístnému bezpečnostnímu kódu karty CVV (na podpisovém proužku). Tento případ je jen další v dlouhé řadě. Pouhé tři týdny před tím CityGroup přiznala, že jí byla zcizena data o 3,9 mil. Držitelů kreditních karet. Data byla na magnetických páscích, které měla přepravní firma UPS převést nákladním autem ze skladu v New Jersey do Texasu ke zpracování. Zásilka nebyla nikdy doručena a přes intenzivní pátrání se nenalezla. Potencionální škoda je značná, neboť vedle finančních informací se ztratila

také čísla sociálního pojištění (Social Security Number), údaj srovnatelný s rodným číslem, pomocí kterého lze získat všechny osobní údaje konkrétní osoby. Od začátku roku se v USA 3,5 mil. lidí stalo obětí zlodějů dat, a zneužití citlivých údajů je tak nejrychleji rostoucí podvod. Dopad na klienty je vedle finanční újmy také psychický. Stále četnější ztráty dat o kartách v USA (např. ve společnosti Choice Point došlo ke krádeži dat na jaře 2005) vyvolaly odezvu a přípravu nové strategie. Např. v Kalifornii schválili nový zákon, který finančním institucím nařizuje zveřejňovat informace o zcizených dat. Většina případů poslední doby tak byla zveřejněna, neboť byli postiženi i držitelé karet v Kalifornii. Kongres USA se také zabývá návrhem, aby povinnost zveřejňování byla rozšířena na všechny státy. Skupiny se zájmem o ochranu osobních dat chtějí jít dále a více regulovat celou oblast zpracování dat s poukazem, že citlivé údaje jsou využívány komerčně mediálními koncerny a obchod s těmito daty narůstá. Na druhé straně lobistické skupiny zpracovatelů dat upozorňují na probíhající samoregulaci a brání se ji nahradit přísnými státními předpisy. Svoji svobodu ve zpracování dat a utajování informací si velice cení, od r. 1998 investovaly do svých lobistických skupin více než National Rifle Association do loby obhajující volná obchod se zbraněmi a jejich držení. Za pouhý 1 dolar prodávají zloději na internetu údaje z ukradených platebních karet, uvádí studie společnosti Symantec. Průzkum probíhal v červenci až prosinci 2006. Kreditní karty z USA včetně vertifikačního čísla jsou k mání za cenu 1 do 6 USD, zatímco podrobnosti o identitě majitele včetně čísla účtu a pojištění se provádějí za 14 až 18 USD. Asi polovina všech nabídek zcizených dat pochází z USA. Dostupnost dat o platebních kartách a snadnost výroby jejich duplikátů je velmi lákavá. Podvodnické gangy pak musí získat dostatečné množství „bílých koní“, které desítky duplikátů musí rychle po celém světě přivést do oběhu. Hledají zejména mezi mladými nezkušenými lidmi. Jeden zahraniční student byla za četné úspěšné pokusy výběru hotovosti z bankomatů v Praze již umístěn do vyšetřovací vazby….“

Kanada je jednou ze zemí s nejvíce počítačově gramotným obyvatelstvem na světě. 25 % kanadských domácností má přístup k internetu. Kanada má zřízeno speciální oddělení věnující se boji proti kyberzločinu - *Canadian´s Police´s Information Technology Security Branch*. Kanadská policie absolvuje speciální internetové školení. Nejvyšším dokumentem týkajícím se informační bezpečnosti je *Government Security Policy*, doplněný řadou prováděcích předpisů nazývaných Operational Standards. Velký důraz je kladen na zvyšování úrovně znalostí o informační bezpečnosti (program Information Security: Raising Awareness).

Německo bylo prvním státem, který zvláštní normou upravil otázku odpovědnosti poskytovatelů volného prostoru – *Teledienstegesetz* (TDG) – přijetí tohoto zákona předcházela kauza společnosti *CompuServe Inc.* Německo patří k tradičním zemím, které kladou vysoký důraz na bezpečnost, jíž se věnuje už řadu let. Dokladem je dlouhodobě zdokonalovaný projekt *IT-Grundschutzhandbuch* (Příručka základní ochrany IT), závazný pro organizace veřejné správy a široce přijímaný jako metodické vodítko v komerčních organizacích. Německo má pro boj s EIK různé organizace – jedna se specializuje na organizovaný zločin jako takový, druhá na zločin spojený s ICT. *ZaRD* [38] byla založena v roce 1990 jako specializovaná agentura pro monitorování internetových aktivit, nikoli pro vyšetřování konkrétních případů. Převážná část případů se týká dětské pornografie. [53]

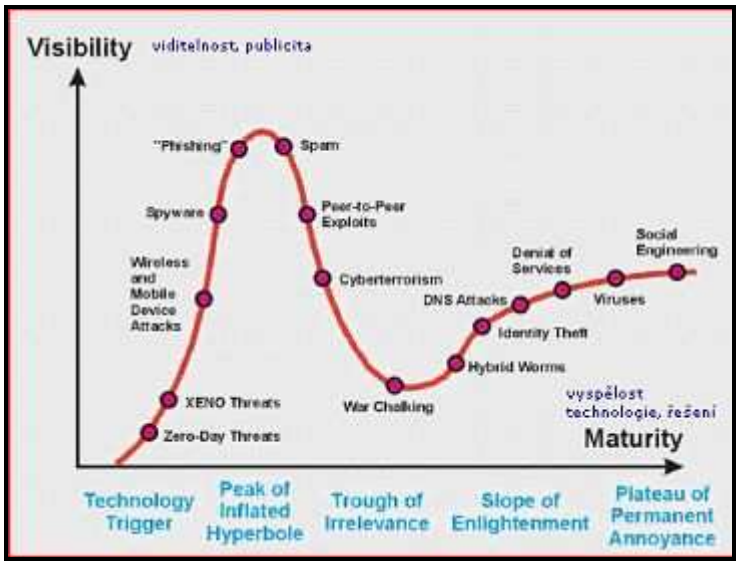
Ve **Spojeném království** stačí k ochraně autorského díla pouhé vytvoření díla a jeho označení značkou copyrightu. *Copyright Act* z roku 1988 stanovuje ochranu počítačového programu, dokonce zde probíhaly úvahy o ochraně SW jako fotografického nebo filmového díla. Ochrana copyrightem byla počítačovému programu přiznána v roce 1985 dodatkem *Copyright (Computer Software Amendment) Act*. Kybernetické trestné činy byly upraveny v *Data Protection Act* z roku 1984 a *Computer Misuse Act* z roku 1990, dodatečně byl vydán zákon *Regulation of Investigatory Powers* (RIP) z roku 2000. Velká Británie je z evropských zemí pravděpodobně nejdále v implementaci informační bezpečnosti – má vypracován systém technických i organizačních opatření v podobě *High-level Information Assurance GESG Policy*.

Jak již bylo mnohokrát zmíněno, internet je globálním médiem bez hranic. Kybernetický zločin ovlivňuje jednotlivce, korporace, ekonomiky i národní bezpečnost všech zemí díky rozšířenosti internetu. Ten předpokládá mezinárodní spolupráci, harmonizaci právních předpisů a vývoj bezpečnostních nástrojů. Spolupráce již mj. probíhá např. mezi výrobci bezpečnostního SW, kteří sdílejí informace o virových nákazách a spywaru z důvodu jednotného boje proti tomuto malwaru. Nutnost úzké **spolupráce** uznávají i zástupci soukromého a veřejného sektoru - ta je charakterizována otevřeností a intenzivní oboustrannou komunikací.

Zajímavý pohled na EIK provedla analytická firma *Gartner*, která jednotlivé hrozby znázornila podle jejich **životního cyklu**, neboť každý jev EIK prochází určitým vývojem. Znázornění míry výskytu dané hrozby, jakési její popularity na časové ose nejlépe vystihuje tzv. *HypeCycle* diagram. Na následujícím obrázku č. 3 můžeme sledovat stav z

[53] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. 97 s. ISBN 80-7226-419-2

konce roku 2004. Svislá osa diagramu (visibility) vyjadřuje míru výskytu hrozby a horizontální osa (maturity) vyspělost hrozby – to znamená, že nejnovější hrozby se nacházejí v levé části horizontální osy, ustálené hrozby v části pravé. Životní cyklus hrozby rozeznává pět vývojových oblastí – některé jevy nemusí projít všemi etapami. Může se stát, že se některé hrozby díky vhodným opatřením či překonání technologie vytratí.



Graf 1- Kybernetické hrozby z konce roku 2006
[zdroj] 16.

V první oblasti tzv. technologických spouštěčů se - jak již název napovídá - vyskytují hrozby, které se objevují s novými technologiemi. Obecně můžeme říci, že jde o novinky na trhu nebo ve sledované oblasti [39]. **Druhou oblastí** je tzv. vrchol zvýšeného zájmu, vrchol očekávání. Sem patří hrozby, o kterých se nejvíce hovoří a je jim věnována maximální pozornost a ochrana. **Třetí oblastí** je tzv. dno irelevantnosti, rozčarování. Do této oblasti řadíme hrozby, o kterých se přestává mluvit, mají svůj vrchol pozornosti za sebou. **Čtvrtou oblast** tzv. svah znovuzrození, renesance tvoří hrozby, které se postupně stávají realitou, jejich výskyt je na denním pořádku. Poslední, **pátou oblastí** je tzv. rovina neustálých zlobičů, kdy se hrozby reálně projevují v běžné praxi. Jsou masově rozšířeny a způsobují díky své vyspělosti závažné problémy.

Můžeme pouze odhadovat, jakým směrem se bude EIK ubírat, nicméně určité - **nepříliš optimistické prognózy** - jsou známy. Ve stručnosti můžeme říci: finančně motivovaní hackeři (black hats) budou využívat stále sofistikovanější metody útoku, a to nejen na softwarové systémy od firmy Microsoft. Podle pracovníků mezinárodní

společnosti *X-Force*[54] postihne nová vlna zájmu hackerů i jednoúčelové servery, modemy a síťové prvky. Podle prognózy dojde ke změně ve způsobu doručování malware, intenzitu napadání podpoří tvůrci virů sériovými variantami útoků. Dále se očekává, že budou sdíleny a vytvářeny nejlepší techniky (tzv. best practices) pro napadání systémů. Pozornost bude věnována automaticky generovaným seznamům, zákaznickým a uživatelským záznamům a požadavkům na informace spolu s odesílanými dávkami dat.

Sociální inženýrství a jeho praktiky budou využívány pro získávání dat na objednávku (zákaznické webové služby, pořizování statistik, individuální parametry vyhledávačů a online formuláře). Nemůžeme opomenout ani napadání mobilních systémů. Škodlivé kódy budou napadat prostředí bezdrátových sítí (Bluetooth, Wi-Fi, GSM, GPRS atd.). Dokonce se mají objevit synchronizované útoky, které napadnou mobilní zařízení i osobní počítač současně.

Dojde-li k naplnění této vize, pak operátoři zaznamenají více než tisíc nakažených zpráv za hodinu. Dále se očekává rozmach tunelování dat a tvorba neviditelných sítí útočníků. Bude docházet k napadání systémů přes zařízení s přímým přístupem k paměti (USB, PCMCIA, diskové řadiče, zvukové karty apod.). Poslední problematickou oblast vidí pracovníci *X-Force* v útocích na DNS servery (pharming). Firmy by proto měly investovat nemalé částky do IB, neboť tyto hrozby mohou zasáhnout kromě jiného klíčové **informační systémy a sítě**. Ty jsou využívány nejen ke komunikaci a obchodu, ale i k provozu důležitých odvětví, jako je zdravotnictví, energetika atd. Zranitelnost těchto systémů se zvyšuje jejich připojením k internetu a dopady útoků na takové systémy pak mohou mít za následek narušení národního hospodářství, v případě kyberterorismu i ztráty na životech, popř. mezinárodní důsledky.

ICT způsobily v našem pracovním i osobním životě velké změny. Vedle usnadnění a zkvalitnění různorodých činností dochází zároveň ke zneužívání technologií, zejména internetu. Ten přináší problémy v rovině technologické,

[54] HLAVENKA, J. *Phishing: Když si hacker podá ruku se zločincem* [online]. 6.7.2004

etické i legislativní a čím dál častěji se stává nástrojem informační kriminality v kybernetickém prostoru. Nejzávažnější problémy tvoří **ztráty důvěrných informací**, které mohou být následně využívány pro další ilegální činnosti, **masové porušování AP** v prostředí internetu, kde vládne naprostá anarchie, a v neposlední řadě i **oblast internetových podvodů a obtěžování**. Důsledkem jmenovaných jevů může být jak ohrožení obchodních aktivit a ztráta soukromí, tak ztracení důvěry uživatelů v ICT. Proto je nezbytné, aby jednotliví uživatelé a společnosti věděli, jakým způsobem může EIK ohrozit jejich informace a data a jakým následkům se v případě nedostatečné připravenosti či ignorance takových jevů vystavují.

Opatření proti EIK by měla být především **preventivního charakteru**. Mělo by být rozšiřováno obecné povědomí o možných hrozbách a následcích EIK. Pro řešení problému EIK je nezbytný **komplexní přístup** – od zajištění bezpečného internetového obchodování, soukromí jednotlivce, zvyšování povědomí o IB až po zahrnutí výuky do studijních plánů policistů, soudců atd. Ale aby se změnilo smýšlení uživatelů o beztrestném kopírování či jiných deliktech, je zapotřebí **spolupráce** institucí soukromého, veřejného i mezinárodního charakteru. Další výzvou je **aktualizace právních předpisů**, které by měly držet krok s dynamickým vývojem ICT a postihovat tak charakter trestných činů v kyberprostoru.

Vyhlídky na vymýcení EIK z našeho života jsou poměrně nerealistické, alespoň ne v dohledné době. V každé společnosti, i té informační, se vždy najdou jedinci, kteří budou obcházet daná etická i legislativně zakotvená pravidla a zneužívat důvěry občanů. Při pomyšlení, že dojde k integraci všech technologií a „virtualizaci“ digitálního prostředí do podoby elektronického domova či kanceláře, můžeme jen čekat, jaké přínosy či nové hrozby tato vize přinese.

Vzhledem k počtu odcizených dat se jedná o značně rozšířenou trestnou činnost. Pachatelé jednak vybírají peníze z bankomatů, ale další formou této trestné činnosti jsou využívání těchto dat při internetové platbě bez přítomnosti platební karty, kdy jsou např. objednávány pobyty v hotelech a následně stornovány s tím,

že zbytek zaplacené částky po odečtení storno poplatku, žádá pachatel převést na svůj účet v bance Western Union nebo Barclays Bank.

V další variantě žádali pachatelé po hotelech zakoupení různého zboží či služeb. V současné době se pachatelé, převážně z Nigerie snaží nakupovat po internetu různé zboží nebo letenky s tím, že toto chtějí zaslat na určenou adresu, nebo si jej pomocí tzv. „ bílých koňů“ vyzvedávají na určeném místě. Objednávky jsou zasílány z nevysledovaných e-mailových adres, často hromadně na větší počet hotelů či obchodních míst.

Přestože v současné době jsou hotely i řada obchodních míst informovány a v řadě případů tyto podvodné objednávky odhalují, přesto se stále najde mnoho obchodníků, kteří se pachateli nechají nachytat.

V této souvislosti je třeba upozornit, že obchodní místo je povinno provádět tzv. autorizace, kdy v řadě případů se zjistí, že transakcí z důvodu zablokování karty nelze provést. Rovněž tak obchodní místo při transakci po internetu, kdy je mu placeno z konkrétního účtu, nesmí zbylé peníze přeposílat na jiný účet, ale vrátit na účet, z něhož mu byly poslány.

K vysvětlení způsobu, jak se hackeři a následně kriminální podsvětí dostalo k datům z platebních karet uvedeme článek z elektronického magazínu Sdružení pro bankovní karty Cardmag. Č. 03/2005
(www.bankovnikarty.cz/data/cm3_2005.pdf.):

5 VÝZKUM ELEKTRONICKÉHO OBCHODOVÁNÍ NA ČESKÉM KAPITÁLOVÉM TRHU

Počet uživatelů různých bankovních služeb v České republice se začal radikálně zvyšovat až po roce 1989. Bankovnictví jako odvětví prochází nyní značnými změnami, a to zejména díky dvěma významným trendům: informační a komunikační revoluci a globalizaci. Banky mění pod vlivem těchto změn svou tvář, investují do inovací, které se pro ně stávají stále důležitější.

Důsledkem těchto tlaků jsou nejenom změny v chování bank vůči klientům a nabízení pestřejších možností komunikace a produktů, ale i změny ve vnitřním chování bank, kdy prostřední nutí banky k daleko dynamičtějšímu chování a uspořádání.

Banky byly po staletí omezeny při komunikaci s klientem na osobní styk zejména prostřednictvím svých poboček a zástupců. V druhé polovině dvacátého století se však díky prudkému technologickému vývoji tato situace velmi razantně mění a finanční instituce mají k dispozici velkou škálu komunikačních prostředků.

Hnacím motorem změn jsou především tyto faktory:

- úspora nákladů je dána snížením variabilních nákladů na jednu transakci. Na druhou stranu je třeba uskutečnit investice, které alespoň krátkodobě zvýší fixní náklady. Banky totiž obvykle nejsou schopny díky zavedení moderních komunikačních prostředků okamžitě ušetřit jiné fixní náklady, například propustit personál nebo zavřít část svých poboček. Tato úsporná opatření mohou následovat až po relativně dlouhé době, pokud banka nechce riskovat ztrátu podstatné části své klientely. Úspora nákladů se tedy projevuje až po určité době, pouze při vyšších objemech, a tedy zejména u těch bank, které operují na velkých trzích nebo globálně.
- dalším hnacím motorem těchto inovací je zatraktivnění služeb pro klienta neboli zvýšení klientem vnímané přidané hodnoty. Určitá část populace vnímá rychlost služeb, kvalitu služeb a úsporu času jako důležitou hodnotu, kterou mu může přinést právě používání těchto moderních prostředků. Velikost této skupiny lidí je v jednotlivých zemích různá a závislá jak na vyspělosti dané země, tak i na kulturních a sociálních tradicích a politických podmínkách. Je například známé, že využívání moderních komunikačních technologií (mobilních telefonů, Internetu) ve Skandinávii je podstatně vyšší něž ve zbytku Evropy, ač ekonomická úroveň jednotlivých zemí je srovnatelná.

Zařazení platebních karet do oblasti přímého bankovnictví nemá zcela jednoznačnou podporu odborné veřejnosti. Lze se setkat s názorem, že platební karta není klasickou

formou komunikace mezi klientem a bankou, neboť jejím prostřednictvím nelze provést jinou operaci než nejtriviálnější platbu.

Podle obecně přijímané definice je platební karta identifikačním dokladem, jejíž rozměry a fyzikální vlastnosti stanoví mezinárodní norma ISO 3544. Na lícové straně je místo pro magnetický proužek (jsou na něm zaznamenány identifikační údaje pro elektronické transakce) a podpisový proužek.

Podle čísla karty lze poznat mnoho věcí. První dvě číslice identifikují druh karty (např. VISA začíná vždy číslem 4, EC/MC pětkou), dalších 5 číslic vydavatele karty (banku), zbytek je určen pro identifikaci konkrétního držitele.

Platební karta je vždy majetkem banky, která ji vydala, nikoli držitele. Z tohoto důvodu peněžní ústavy většinou vyžadují její navrácení po skončení doby platnosti.

S platební kartou lze provádět v podstatě dvě základní věci – platit za zboží a služby nebo vybírat hotovost z bankomatu. Karta by se vzhledem ke svému názvu měla využívat především k placení a nikoli pro výběry z bankomatu. Pro vlastníka karty je bezpečnější, pohodlnější a hlavně výhodnější platba kartou, jelikož náklady transakce nese obchodník, který dostane o určité procento nižší částku.

5.1 KVANTITATIVNÍ VÝZKUM POTENCIONÁLNÍCH RESPONDENTU

Na základě výše uvedených kritérií bylo vybráno 140 respondentů, kteří byli v rámci primárního výzkumu kvantitativního charakteru osloveni, a to buď formou dopisu s přiloženým dotazníkem nebo prostřednictvím osobního setkání s nimi. V následující tabulce je uvedena četnost jednotlivých způsobů oslovení, včetně míry návratnosti dotazníků.

ÚDAJE O DOTAZNÍKOVÉM ŠETŘENÍ	ZPŮSOB OSLOVENÍ VYBRANÝCH RESPONDENTŮ		CELKEM
	Dopis	**Osobní setkání**	
Počet předaných dotazníků	95	45	140
Počet vrácených dotazníků	48	36	84
Míra návratnosti dotazníků	**50,5%**	**80%**	**60%**

Tabulka 1 - Počet dotazníků použitých pro primární výzkum a míra jejich návratnosti

[zdroj] Vlastní zpracování

Z tabulky je patrné, že z celkového počtu 140 předaných dotazníků jich bylo vráceno a následně vyhodnoceno 84, což představuje 60% jejich návratnosti. Nejvyšší míry návratnosti 80% bylo dosaženo při osobním setkání .

Formulace otázek v dotazníku byla zvolena tak, aby umožňovala:

- volitelné odpovědi formou výběru z nabízených variant
- výběr odpovědí *ano* či *ne*
- odpovědi vyžadující uvedení konkrétního číselného údaje
- doplňkové a volné odpovědi

Pro přehlednost je vždy nejprve uvedena otázka z dotazníku a dále následuje počet odpovědí na nabízené možnosti a odpovědi bez vyjádření. Převažující odpověď je vždy zvýrazněna.

1. Jste držitelem platební karty?	Celkem odpovědí		84	%
	Z toho:	**Ano**	**68**	**80,9**
		Ne	16	19,1
		bez vyjádření	0	0

Tabulka 2

[zdroj] Vlastní zpracování

Závěr: Výzkum prokázal, že většina zkoumaných respondentů považuje platební kartu za součást moderního obchodování .

2. Víte, jaké jsou výhody debetních karet oproti hotovostním platbám?	Celkem odpovědí		84	%
	Z toho:	**Ano**	**71**	**84,5**
		Ne	13	15,5
		bez vyjádření	0	0

Tabulka 3

[zdroj] Vlastní zpracování

Závěr: Většina zkoumaných respondentů uvádí, že jsou dostatečně informováni o možnostech výhod platbou debetní kartou oproti hotovosti.

3.Považujete čipovou kartu za bezpečnější?	Celkem odpovědí		84	%
	Z toho:	**Ano**	**70**	**83,4**
		Ne	14	16,6
		bez vyjádření	0	0

Tabulka 4

[zdroj] Vlastní zpracování

Závěr: V rámci provedeného výzkumu bylo zjištěno, že 83,4% dotázaných považuje čipovou technologii za bezpečnější.

4.Znáte možnosti funkčnosti Vaší platební karty?	Celkem odpovědí		84	%
	Z toho:	**Ano**	**59**	**70,2**
		Ne	15	17,8
		bez vyjádření	0	0

Tabulka 5

[zdroj] Vlastní zpracování

Závěr: Provedený průzkum prokázal, že většina zná možnosti funkčnosti platební karty.

5. Považujete dle Vašeho názoru umístění ochranných prvků za dostatečné?	Celkem odpovědí		84	%
	Z toho:	**Ano**	**63**	**75**
		Ne	21	15
		bez vyjádření	0	0

Tabulka 6

[zdroj] Vlastní zpracování

Závěr: Z výsledků výzkumu je patrné, že většina dotázaných 75% považuje umístění ochranných prvků za dostatečné.

6. Pokud byste se dostali do pokročilého věku, báli byste se moderních vymožeností ?	Celkem odpovědí		84	%
	Z toho:	**Ano**	**59**	**70,2**
		Ne	25	29,8
		bez vyjádření	0	0

Tabulka 7

[zdroj] Vlastní zpracování

Závěr: V rámci provedeného výzkumu bylo zjištěno, že 70,2 % dotázaných by se moderních technologií nebálo.

7. Byly jedním z důvodů legislativní překážky?	Celkem odpovědí		84	%
	Z toho:	Ano	7	8,3
		Ne	**66**	**78,5**
		bez vyjádření	11	13,2

Tabulka 8

[zdroj] Vlastní zpracování

Závěr: Většina zkoumaných respondentů uvádí, že legislativní překážky u většiny zkoumaných nebyli důvodem.

8. Byly jedním z důvodů administrativní překážky?	Celkem odpovědí		84	%
	Z toho:	ano	13	15,5
		Ne	**62**	**73,8**
		bez vyjádření	9	10,7

Tabulka 9

[zdroj] Vlastní zpracování

Závěr: Většina zkoumaných respondentů uvádí, že administrativní překážky, podobně jako překážky legislativní, nepředstavují pro většinu zkoumaných respondentů hlavní důvod.

9. Setkali jste se ještě s nějakými jinými problémy?	Celkem odpovědí		84	%
	Z toho:	ano	12	14,2
		ne	**65**	**77,3**
		bez vyjádření	7	8,5

Tabulka 10

[zdroj] Vlastní zpracování

Závěr: V rámci provedeného šetření uvedlo pouze 14,2 % zkoumaných, že se při rozhodování setkaly také s jinými problémy. Jednalo se například o dlouhé čekací doby při realizaci vyřízení náležitosti platební karty.

10. Byla jedním z důvodů nedostatečná informovanost o možnostech a výhodách platby platební kartou ?	Celkem odpovědí		84	%
	Z toho:	**ano**	**36**	**42,9**
		ne	27	32,1
		bez vyjádření	21	25

Tabulka 11

[zdroj] Vlastní zpracování

Závěr: Z výsledku průzkumu je patrné, že většina dotázaných (42,9 %) nebyla dostatečně informována o možnostech a výhodách platby platební kartou.

11. Je naše společnost dostatečně informována o možnostech zneužití platební karty?	Celkem odpovědí		84	%
	Z toho:	ano	11	13
		ne	**57**	**67,9**
		bez vyjádření	16	19,1

Tabulka 12

[zdroj] Vlastní zpracování

Závěr: V rámci provedeného výzkumu bylo zjištěno, že 67,9 % dotázaných si myslí, že naše společnost není dostatečně informována o možnostech zneužití platební karty.

5.2 ZHODNOCENÍ VÝSLEDKŮ VÝZKUMU

Terénní sběr dat jsem provedl ve Vyšší policejní škole MV v Brně. Byly získány údaje od 84 respondentů, tj. policistů studujících na této škole a občanských zaměstnanců. Zkoumaný soubor se skládal ze 61 mužů (72,6 %) a z 23 žen (27,4 %). Bylo v něm 77 % svobodných, 21 % ženatých/ vdaných a 2 % rozvedených respondentů. Věk dotazovaných se pohybuje od 19 do 43 let. Co se týká dokončeného stupně vzdělání, 64 % respondentů udalo střední školy zakončené s maturitou, 36 % respondentů mělo vysokoškolské vzdělání.

Na základě výše uvedených výsledků primárního výzkumu lze konstatovat, že většina dotázaných respondentů v současné době považuje český kapitálový trh za potenciální zdroj pro financování svého rozvoje. Přestože většina zkoumaných je přesvědčena o tom, že bez platební karty se v současně době neobejdou, dostatečná informovanost o možnostech zneužití platební karty je velmi malá.

5.3 OSTATNÍ PŘÍČINY

Jednoznačně zde chybí národní, respektivně. mezinárodní systém[55], který by oblast platebních karet centrálně zastřešoval, obdobně jako u padělaných bankovek a mincí (systém centrálních bank, národní specializované policejní útvary, vč. uzavřených smluv o vzájemné spolupráci) atd. Např. v Polsku existuje jednotný elektronický systém centrálního monitorování aktivit uskutečněných transakcí na bankomatech. Na rozdíl od Polska, je v ČR, kde je x-různých subjektů zabývajících se monitoringem transakcí, některé banky přitom nemají žádný systém, některé banky mají vlastní systém videozáznamů na bankomatech, některé nemají bankomaty osazené videokamerou vůbec, někde tuto činnost za úplatu vykonávají další soukromé subjekty apod. V ČR je možné žádat u bankovního sektoru o monitoring pohybu platebních karet a uskutečněných transakcí, ale tímto se pro různé banky[56] zabývají čtyři různé subjekty za úplatu a některé banky nemají možnost monitoringu vůbec. V řadě případů požadavků na technický monitoring či získání informací bez uvádění výše bankovního konta, jména a adresy uživatele platební karty či dalších osobních dat. Vyžadují banky povolení a příkazy státních zastupitelství a soudů k vydání jakýchkoliv technických údajů apod., přičemž se odvolávají na subjektivní právní názory a výklady zákonů svých právních oddělení.

[55] HRADECKÝ, M. *Platební prostředky jejich ochrana a padělání*.Praha 2008.ISBN 80-7312-055-0
[56] Zákon České národní rady č. 6/1993 Sb., o České národní bance ve znění následně vydaných novel

Velkým problémem je získat nejen operativně informace z bankovního sektoru, ale i operativní zajištění videozáznamů z bankomatů.

Dalším problémem, tentokrát v rámci policie ČR, je nedokonalost vlastních struktur. Spolupráce odboru padělání s expoziturami ÚOOZ v teritoriu je na dobré úrovni, obdobně lze hodnotit spolupráci s odborem hospodářské kriminality (dále jen OHK) jednotlivých krajských správ, vyjma hl.m. Prahy a částečně i OHK Středočeského kraje, kde dochází k prodlevám při vypracovávání žádostí o zjištění informací dle čísel IMEI, SIM karet, buněk, ale i předání zajištěných skimmovacích zařízení k znaleckému zkoumání, nemluvě o tom, že kapacity Kriminalistického ústavu v Praze (dále jen KÚP) a oddělení kriminalistických a technických expertíz(dále jen OKTE) jsou přetížené, resp. nedostatečné a dodací termíny jsou až jeden rok. Z tohoto důvodu byla např. odborem padělání předávána v roce 2007 po dohodě s BLKA Mnichov zajištěné skimmovací zařízení na tamější policejní znalecký ústav a tento ve lhůtě cca jednoho měsíce zasílal výsledky zkoumání. Další existující problém (přes snahy odboru padělání na úseku různých instrukčně-metodických zaměstnání (IMZ) a proškolování), je nedostatečné v informovanosti řadových policistů v běžném výkonu, kteří neznají důkladné postupy v případě zjištění skimmovacích zařízení na bankomatech, resp. při zjištění podezření na výskyt pachatele provádějícího výběry peněz na padělané platební karty.

Nemalým problémem je i materiálně technické vybavení odboru padělání, resp. policistů ÚOOZ zařazených na expoziturách potřebným hardware a software pro práci na úseku platebních karet. Než vyjmenovávat, co chybí, je jednodušší uvést, že ze speciálního zařízení a software vlastní odbor padělání prostřednictvím sponzorského daru jednu čtečku dat z magnetického proužku s nefunkčním software k připojení k PC a jeden zastaralý pokladní terminál na 220V, s nímž je možné přečíst data z magnetického proužku karty (chybí však návod k použití, nelze nastavit čas na terminálu, akubaterie je vadná, dochází náplň na tisk apod.). Pokud je nám známo, jednu čtečku platebních karet k připojení na PC vlastní jako sponzorský dar i OHK hl.m. Prahy. Ač potřebný software a hardware byl vyžadován, nebyl dodán. Např. pokladní terminál je v případě potřeby zapůjčován i na expozitury ÚOOZ, neboť vybavení OHK na krajském a okresním stupni je takové, že když v Ústí nad Labem bylo třeba po zadržení pachatele zjistit, zda členské karty obchodního řetězce, které měl u sebe, byly použity jako platební karty k výběru peněz a zda se jedná o padělek, použili policisté dvě karty v bankomatu k výběru minimální možné částky 200,-Kč. Protože se podařilo tuto částku vybrat, bylo zjištěno, že se jedná o funkční padělek platební karty.

5.4 STANOVENÍ ZÁKLADNÍCH PŘEDPOKLADŮ PRO BEZPEČNOST PLATEBNÍCH KARET

5.4.1 Překážky legislativního charakteru

Bezpečnostní rizika na úseku padělání bezhotovostních platebních prostředků – platebních karet vyplývají zejména z nedokonalosti stávajícího[57] zákona č.140/1961Sb., který je koncipován především tak, aby postihl padělání platebních prostředků - papírových bankovek a mincí - dle mezinárodní Úmluvy o potírání penězokazectví (Ženeva 20.4.1929), vyhlášené ve Sbírce zákonů č. 15/1932 Sb., přičemž stejný problém zůstal i ve zpracované a neschválené rekodifikaci trestního zákona.

V trestním zákoně ve znění následně vydaných novel jsou sice uvedeny trestné činy týkající se padělání peněz, konkrétně § 140 – padělání a pozměňování peněz, § 141 – udávání padělaných a pozměněných peněz, § 142 – výroba a držení padělatelského náčiní, ale pouze § 143 (společné ustanovení) hovoří obecně o tom, že stejná ochrana se kromě jiného poskytuje též tuzemským a cizozemským bezhotovostním platebním prostředkům. Přitom nebyl použit ani § 89 zabývající se tzv. výkladem pojmů používaných v trestním zákoně k výkladu, jakým způsobem se ochrana ze zákona vztahuje i na padělané platební karty. Nebyly do zákona doplněny odkazy např. na zákon České národní rady č.6/1993 Sb., o České národní bance, příp. Vyhláška České národní banky č. 36/1994, a již vůbec na zákon č. 21/1992 Sb., o bankách, či zákon č. 124/2002 Sb., o platebním styku, ve znění následně vydaných novel, Věstník ČNB částka 10/2004, výklad k vybraným ustanovením zákona o platebním styku nebo Směrnice EU č.2000/46/ES a č.97/7/ES a Doporučení EU č.97/489/ES.

Stávající legislativa je tedy nastavena vcelku precizně na ochranu peněz, ale ne **na ochranu bezhotovostních platebních prostředků.** Vzhledem k tomuto stavu orgány činné v trestním řízení, zejména někteří státní zástupci a soudci nepoužívají při aplikaci konkrétního paragrafu pro postih pachatelů, kteří padělají platební karty, trestné činy proti měně, ale využívají trestný čin neoprávněného držení platební karty (§ 249b) trestního zákona, přičemž tento paragraf byl do trestního zákona zařazen pro postih pachatelů, kteří odcizí platební kartu (důvodem je nejasná formulace v tomto paragrafu týkající se slov: „…nebo předmět způsobilý plnit její funkci,….“).

Obecně lze konstatovat, že současný technický vývoj na úseku bezhotovostních platebních prostředků (zejména u platebních karet či virtuální platby platební kartou po

[57] Zákon č. 140/1961Sb., trestní zákon ve znění následně vydaných novel

Internetu atd.) předstihl právo. Přitom padělání bezhotovostních platebních prostředků (zejména platebních karet) či uvádění a zneužívání odcizených dat z platebních karet při platbách na Internetu v současné době je značně rozšířenou trestnou činností a lze předpokládat, že s dalším rozšiřováním používání platebních karet i plateb přes Internet bude docházet i k dalšímu rozšíření této trestné činnosti.

Na základě výše uvedeného nyní dochází k nejednotnému postupu a vzhledem k tomu, že ochranu je třeba ve smyslu §143 trestního zákona poskytnout všem platebním prostředkům, je třeba trestní zákon novelizovat.

5.4.2 Vliv bankovního sektoru na bezpečnost karet

.

K značnému nárůstu trestné činnosti páchané organizovanými skupinami pachatelů došlo v roce 2007 z hlediska skimmování dat z platebních karet a PIN na bankomatech v ČR, následné výrobě padělků karet a výběrům finanční hotovosti na bankomatech v ČR i zahraničí. Různé skupiny pachatelů v období roku 2007 např. nasadily na bankomaty skimmovací zařízení v cca 84 případech v různém časovém období, často i ve více dnech po sobě nebo opakovaně a následně docházelo k výběrům peněz na padělané platební karty jak v ČR, tak v zahraničí. Celkem bylo napadeno 45 různých bankomatů, často opakovaně. V prvním pololetí zejména bankomaty ČS, GEMB, EBanky a KB, v druhém pololetí zejména GEMB.

Zneužívání pokladních terminálů ke skimmování dat z platebních karet dosud značně rozšířené v Evropě, zatím nebylo na území ČR zjištěno.

Bankovní sektor se v značné míře spoléhá na zvýšení bezpečnosti platebních karet zaváděním čipové technologie, avšak v současné době v ČR neexistuje 100% zavedení této technologie na platebních kartách, bankomatech a pokladních terminálech a stále jsou používány tzv. hybridní platební karty, tedy s čipem i magnetickým proužkem. Informace z Francie varují, že ani čipová technologie nemusí být 100% ochranou proti padělání platebních karet.

Ke klasickému získávání dat z platebních karet prostřednictvím hackerů (jako v USA, Ukrajina, apod.) a celosvětové sítě Internet na území ČR zatím nedošlo, pouze nezjištění pachatelé v několika případech napadli formou phishingu a pharmingu webové stránky některých bank v ČR (KB, Citibank a ČS) s tím, že následky byly bankovním sektorem eliminovány. Stále přijíždí, resp. projíždí ČR skupiny i jednotlivé osoby, které provádí

výběry peněz na bankomatech na padělané karty, jejichž data byla naskimmována v zahraničí nebo získána zahraničními hackery na Internetu.

K obdobnému nárůstu došlo i na úseku používání platebních karet bez jejich přítomnosti[58] (elektronické bankovnictví) prostřednictvím Internetu a faxu, a to zejména organizovanými skupinami pachatelů zejména z Nigerie a Pobřeží Slonoviny, které se takto snaží získávat výběry finančních částek nebo zboží na základě zneužití dat z platebních karet oprávněných držitelů. Zde je velmi často využíváno rovněž padělaných šeků, přičemž v obou případech je značně nesnadné až nemožně vysledovat pachatele mimo území ČR.

Varující je fakt, že organizované skupiny pachatelů jak u skimmingu, tak u internetové kriminality ke své činnosti využívají osob stejné národnosti, jimž byl povolen pobyt na území ČR za účelem např. sloučení rodiny, přičemž původní důvod sloučení nikdo řádně po udělení trvalého pobytu nekontroluje a podmínky udělení jsou oproti jiným státům značně benevolentní.

Přestože rostou počty vydávaných a užívaných[59] platebních karet v ČR (v roce 2002 cca 5,3 milionů karet a v roce 2006 cca 7,9 milionů karet) a stamiliardové převody finančních částek prostřednictvím různých transakcí s platebními kartami (v roce 2002 cca 51,5 miliardy Kč a v roce 2006 cca 166 miliard Kč), jsou bezpečnostní rizika na úseku padělání platebních karet dosti značná. Svůj díl zde má jak bankovní sektor, tak policie, ale i stát jako takový (justice).

V ČR jsou bankami vydávány převážně karty systémů MasterCard a Visa, v menší míře American Express, nejméně a s klesajícím trendem domácí karty vlastních, tzv. „proprietárních“ systémů. Z nebankovních karet zahrnují statistiky v současné době karty Diners Club vydávané v ČR a karty společnosti CCS.

Vývoj počtu vydaných, tzv. aktivních karet (karty, které jsou evidovány v databázích vydavatelů jako použitelné) podávají následující tabulky a grafy:[zdroj][60]

[58] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku) ve znění zákona č. 257/2004Sb.
[59] Věstník České národní banky10 z 19.5.1994 jímž se vydává Úřední sdělení ČNB – výklad k vybraným ustanovením zákona o platebním styku
[60] HRADECKÝ, M. *Platební prostředky jejich ochrana a padělání.*Praha 2008.ISBN 80-7312-055-0

Rok	2002	2003	2004	2005	2006
Počet karet celkem	5 296 067	6 373 591	6 867 733	7 390 357	7 865 227
Z toho: debetní	5 194 057	5 829 857	5 873 728	6 418 446	6 603 621
kreditní	97 629	203 274	372 933	971 911	1 261 606
čipové	800 551	1 428 732	2 166 418	2 830 302	3 488 627

Tabulka 13 - Počty vydávaných karet

[zdroj] 20.

Rok	2002	2003	2004	2005	2006
Počet plateb	35 815 952	67 652 432	83 493 644	99 756 686	116 890 828
Objem plateb (tis.Kč)	42 484 356	77 588 299	91 727 996	114 584 198	133 746 846
Průměrná platba (Kč)	1 503	1 186	1 147	1 099	1 144

Tabulka 14 - Platby kartou u obchodníků**:**

[zdroj] 20.

Rok	2002	2003	2004	2005	2006
Počet plateb	42 500 466	80 373 983	99 072 963	120 342 199	137 414 580
Objem plateb (tis. Kč)	51 442 121	92 558 911	117 977 852	142 735 769	165 619 320
Průměrná platba (Kč)	1 210	1 152	1 191	1 186	1 205

Tabulka 15 - Vývoj počtu a objemu plateb domácími i zahraničními kartami v obchodních místech v ČR

[zdroj] 20.

Ze strany bankovního sektoru kromě již uvedeného 100% přechodu na čipovou technologii např. chybí preventivní kontroly bankomatů, chybějí vnitřní, resp. vnější videokamery na bankomatech, jsou nekvalitní a nejednotné použité videotechnologie a špatné nastavení kamer, ale i nejednotná a v některých případech i chybějící, možnost kvalitního on-line sledování autorizací apod., o evidenci padělaných platebních karet nemluvě.

Stejný problém z hlediska zavedení a pravidelného aktualizování evidence padělaných platebních karet, ale i padělaných šeků, příp. padělků dalších bezhotovostních prostředků existuje u policie[61], i když první kroky z iniciativy odboru padělání na úseku padělaných karet již byly učiněny. Dalším problémem je nedostatečné či chybějící personální a materiálně technické vybavení jak odboru padělání ÚOOZ a pracovníků zabývajících se padělaním na expoziturách ÚOOZ v krajích (vyjma Prahy a Středočeského kraje, kde tuto funkci s nedostatečných počtem tabulkových míst, ale i obsazením tabulek zkušenými odborníky na úseku operativy a výpočetní techniky plní odbor padělání), tak dalších specializovaných policejních složek (OHK) na úseku boje proti padělání platebních karet. Závažným problémem v budoucnu mohou pro policii být např. dosud neexistující počítačoví odborníci na internetovou kriminalitu na úseku padělání platebních karet a šeků.

Z hlediska státu, konkrétně justice je problémem stávající trestní zákon (padělek x náhražka, §140 a násl. x §249b), ale i připravovaná novela, kde nedošlo zatím ani na základě zásadních připomínek odboru padělání k zlepšení, spíše došlo k zakonzervování stávajícího stavu, možná i k zhoršení. K částečnému pokroku, který však není samospasitelný, došlo díky iniciativě odboru padělání na Nejvyšším státním zastupitelství vydáním Obecně závazného pokynu NSZ č. 2/2007, který se snaží řešit dřívější nejednotné postupy státních zástupců ve věci posuzování padělku karty a to, zda tento čin podřadí pod padělání měny (§140 trestního zákona a násl.) nebo jen jako neoprávněné užití platební karty dle §249 písm.b trestního zákona Pochopitelně tento pokyn není již závazný pro soudy a jejich rozhodování nelze předjímat. Celý problém nevznikl jen jedním komentářem v trestním zákonu, ale je celým souhrnem problémů (např. nesrozumitelné zákony o platebním styku, zákony o bankách, nejednotná terminologie v zákonech, chybějící vzájemné propojení příslušných zákonů apod.).

Obecně lze na závěr konstatovat, že zejména vzhledem ke zvětšujícímu počtu vydaných a používaných platebních karet, neukončenému přechodu na čipovou

[61] ZPPP ČR č. 81/2003, kterým se upravuje postup policie ČR při prověřování a vyšetřování trestných činů v případech výskytu penězokazectví ve znění následně vydaných novel

technologii, bezvízovému styku v EU a v dalších státech a volnému průjezdu a průchodu v rámci Schengenského prostoru, zanedbávání prevence ze strany bankovního sektoru, včetně nerespektování potřeb policie na úseku padělání platebních karet, stagnující činnosti policie na úseku padělání šeků (na zaslaná dožádání některé země vůbec nereagují, nelze zjistit majitele uváděných telefonů, nelze zjistit místo ani uživatele mailových adres, celková anonymita Internetu apod.) Bude nadále docházet ve větší míře k nárůstu trestné činnosti organizovaných skupin pachatelů, a to jak na úseku klasického, dnes již známého padělání platebních karet, tak v rámci elektronického bezhotovostního styku prostřednictvím Internetu. V blízké budoucnosti lze očekávat další nové formy a způsoby stávající trestné činnosti, ale i zcela nové (např. zneužívání pokladních terminálů jejich nezákonnými úpravami) a ve výhledu je třeba očekávat i problémy s čipovou technologií.

5.4.3 Skimming platebních karet v roce 2007

Skimming platebních karet, tři slova, za nimiž se skrývá rozsáhlá[62] trestná činnost převážně organizovaných skupin pachatelů s mezinárodním prvkem, zčásti latentní a téměř vždy vzhledem k svému charakteru velice špatně odhalitelná a pokud již dojde k zadržení pachatele, jedná se většinou o poslední článek v organizované skupině.

Vzhledem k masivnímu nárůstu počtů nasazovaných skimmovacích zařízení v České republice v roce 2007 oproti předcházejícím létům (viz. graf č.1) a prováděným opatřením zejména ze strany odboru padělání - Národní centrály proti penězokazectví Útvaru pro odhalování organizovaného zločinu služby kriminální policie a vyšetřování Policie ČR (dále jen „odboru padělání ÚOOZ“), včetně velice úzké spolupráce s Europolem, Interpolem, ale i specializovanými národními policejními útvary některých členských zemí Evropské unie, bylo možné získat pozitivní, ale i negativní zkušenosti v této oblasti.

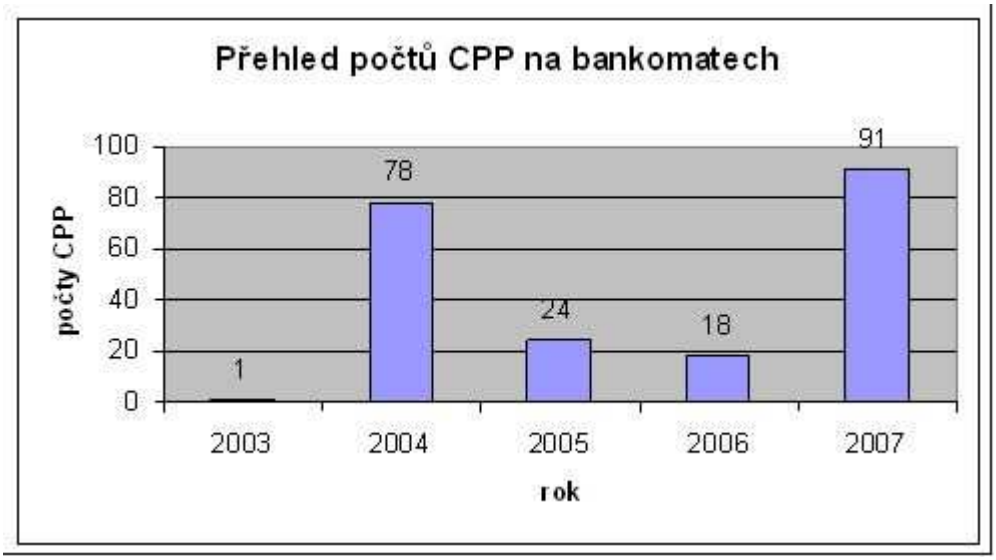
Protože neexistuje oficiální ani neoficiální přehled počtů vyrobených a použitých padělků platebních karet na území České republiky ani nikde jinde ve světě, nelze žádný podobný graf jako výše uvedený zpracovat a případné odhady by byly zcela neobjektivní.

---

[62] HRADECKÝ, M.*Platební prostředky jejich ochrana a padělání*.Praha 2008.ISBN 80-7312-055-0

Důvodem je i to, že na data naskimmovaná v České republice z platebních karet tuzemských i cizozemských vydavatelských bank jsou vybírány finanční částky jak v České republice, tak v zahraničí.

Záměrně se nebudu zabývat právní stránkou problematiky skimmingu platebních karet v České republice, ale zaměřím se na praktickou stránku zjišťování a odhalování pachatelů této trestné činnosti a souvisejících činností.



Graf 2 - Přehled počtů napadených bankomatů
[zdroj] 20.

Poznámka zpracovatele: Napadený bankomat skimmovacím zařízení označuje bankovní sektor zkratkou „CPP“. Neexistuje žádná oficiální centrální evidence počtů napadených bankomatů, pro alespoň orientační zpracování přehledu napadených bankomatů v České republice bylo využito vlastních podkladů České spořitelny do listopadu 2007 (zahrnuty bankomaty České spořitelny i ostatních bank v České republice).

5.4.3.1 Skimming

Pod tento pojem lze zařadit zejména :

1) trestnou činnost páchanou výrobou, držením a v neposlední řadě nasazováním různých speciálních zařízení na bankomaty nebo do bankomatů či pokladních terminálů za účelem získání dat z magnetického proužku platební karty a použitého PIN kódu uživatelem karty
2) trestnou činnost páchanou výrobou, držením a používáním padělků platebních karet při výběrech finančních částek z bankomatů

3) trestnou činnost páchanou tzv. ekonomickými hackery na Internetu, kteří získávají různými způsoby např. data z magnetického proužku platebních karet, příp. další citlivá data, včetně kódu PIN, příp. tento dosud nezjištěným způsobem dekódují a následně data prostřednictvím Internetu prodávají
4) trestnou činnost páchanou prostřednictvím Internetu nebo faxu v rámci internetového bankovnictví, kdy výše uvedenou trestnou činností získaná data jsou zasílána různým hotelům, internetovým obchodům a dalším poskytovatelům zboží a služeb za účelem nákupu služeb, zboží atd.
5) trestnou činnost páchanou získáváním dat z čipů platebních karet a jejich následným přenosem na magnetické proužky padělaných platebních karet s následnými výběry finančních částek na tyto padělky v bankomatech
6) trestnou činnost páchanou různými kombinacemi výše uvedených trestných činností a operativní variabilitou pachatelů

Problém je v tom, že pachatelé nasazují skimmovací zařízení na bankomaty či pokladní terminály kdekoliv na světě, padělky platebních karet vyrábí bezprostředně po získání potřebných dat rovněž kdekoliv na světě a k použití padělků platebních karet dochází rovněž kdekoliv na světě a často i v dosti velkém časovém odstupu od získání dat. Organizované skupiny pachatelů vznikají na národnostním principu, ovládají konspiraci a umí se chránit dosti úspěšně proti sledování apod. Navíc bylo zjištěno, že data získávají pachatelé i prostřednictvím[63] hackerů na Internetu. Nemluvě již o tom, že prostřednictvím Internetu komunikuje řada pachatelů mezi sebou (např. vlastní šifrovaný a zakonspirovaný program CarderIM fungující na stejné bázi jako ICQ, Instant Messenger apod.), a to jak při koupi dat z platebních karet (např. lze zakoupit data z magnetického proužku karty a kód PIN za částku 200,- až 300,- USD za jednu kartu), tak i při přenosu těchto dat prakticky na kterékoliv místo na světě a v neposlední řadě je Internet pachateli zneužíván přímo k trestné činnosti (např. zneužívání internetového bankovnictví).

5.4.3.2 Základní potřeby ke skimmování

Pachatelé potřebují k nejjednoduššímu způsobu naskimmování data z platební karty na bankomatu:

[63] VONDRUŠKA, P. Hackeři, crackeři, rhybáři a lamy. *Cryptoworlds* [online]. 2004, č. 7-8, s. 4-12. [cit. 2004-12-16]

- skutečný vzhled, použité barvy, potisky a rozměry vytipovaného bankomatu, které získají vyfotografováním, natočením na video a změřením
- materiál a elektronické součástky na výrobu falešných nástavců, které lze rovněž běžně získat (např. barvy, sklolaminát, samolepicí oboustranné pásky, kovové desky, běžné akubaterie z mobilů a baterie, čipy a další elektronické součástky, snímač dat z magnetického proužku atd.)
- s běžnou manuální zručností a znalostmi elektroniky poté vyrobí falešné nástavce – skimmovací zařízení a nasadí na bankomat s tím, že funkčnost tohoto zařízení odzkouší pomocí tzv. testovacích karet (např. běžné klubové karty čerpacích stanic nebo i pravé platební karty vlastní či odcizené)
- nasadit na vytipovaný bankomat skimmovací zařízení a jím získaná data ukládat přímo do elektroniky v tomto zařízení nebo je přenášet bezdrátově do přijímacího zařízení (např. pomocí technologie bluetooth nebo jiného bezdrátového spojení do mobilu, notebooku nebo pomocí sms na mobil apod.)
- po určitém časovém období (např. jedné hodiny až několik dnů) skimmovací zařízení z bankomatu sejmout a nasadit na jiný bankomat

5.4.3.3 Pokladní terminál jako nástroj trestné činnosti

V případě skimmování dat z platebních karet[64] na pokladním terminálu, které se dosud v České republice nevyskytlo (pouze byly získány informace o pokusech získat vhodnou osobu uvnitř prodejního místa), ale v jiných zemích Evropské unie byl tento způsob už použit:

- zakoupit vhodný pokladní terminál např. na burze nebo jej přímo odcizit z obchodního místa (čerpací stanice, hotelu, obchodu atd.)
- provést jeho vnitřní úpravu z hlediska elektroniky tak, aby fungoval jako normální terminál a navíc zaznamenával potřebná data na vloženou „tajnou“ elektroniku
- provést výměnu pravého pokladního terminálu za upravený pomocí utajeného vloupání do objektu a obyčejnou výměnou, nebo pomocí falešných servisních techniků příp. pomocí podplacené osoby uvnitř prodejního místa
- po určitém časovém období (např. až jednoho měsíce) upravený pokladní terminál opět vyměnit nebo jednoduše odcizit

[64] Zákon č. 124/2002 Sb., *o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech* (zákon o platebním styku) ve znění zákona č. 257/2004Sb.

5.4.3.4 Získávání dat pomocí hackerů

Pokud jde o získávání dat pomocí hackerů, jedná se o nelegální proniknutí do počítače nebo počítačové sítě a odcizení zde uložených dat platebních karet (např. u firmy zabývající se výrobou pravých platebních karet z dat dodaných vydávajícími bankami) s následným rozkódováním kódu PIN a poté prodejem dat dalším „zájemcům“, kteří si buď vyrobí padělky platebních karet, které použijí k výběrům finančních částek na bankomatech nebo data zneužijí při nákupech pomocí internetového bankovnictví. Druhým způsobem získání dat hackery pomocí internetu jsou různé způsoby[65] phishingu, pharmingu atd., kdy jsou data získávána pomocí falešných stránek od důvěřivých občanů, nebo opět pomocí neoprávněného vniknutí do počítače občana a stažení, zde uložených citlivých dat nebo pomocí falešného mailu obelstění občana (uživatele internetového bankovnictví a získání citlivých dat vstupních kódů, hesel apod.) s tím, že získaná data jsou využívána stejně, jako u předchozího způsobu.

V tomto případě potřebuje pachatel k získání dat počítač nebo notebook se speciálním software nebo znalostmi k jeho tvorbě (např. různé trojské koně, viry atd.) a v pohodlí vlastního domova nebo internetové kavárny na kterémkoliv místě světa s napojením na Internet může v klidu „pracovat“.

5.4.3.5 Výroba platební karty - padělání

- počítač, notebook nebo jiné obdobné elektronické zařízení se speciálním software k čtení a zápisu dat na magnetický proužek a čtečku, resp. zařízení na zápis dat na magnetický proužek
- dále buď jakoukoliv nepotištěnou normalizovanou kartu s magnetickým proužkem (tzv. „bílý plast“), nebo použitou klubovou, vstupní kartu nebo odcizenou platební kartu
- pokud chtěl pachatel dříve nebo chce nyní vyrobit padělek karty se všemi náležitostmi, potřebuje i speciální tiskárnu na potisk karty, hologram a příp. speciální strojek na vytvoření embosovaných čísel (tj. vyražených čísel). Vzhledem k tomu, že bankomaty nemají možnost v současné době kontrolovat při transakci nic jiného než rozměr karty a přečíst data na magnetickém proužku, pachatelé ve většině případů tento drahý způsob výroby kompletního padělku nepoužívají.

[65] PŘIBYL, T. *Po phishingu přichází pharming*. *Computerworld*. 2005, č. 27, s. 28-29

5.4.3.6 Překážky technického charakteru

Dalším negativním faktorem je skutečnost, že zatím neexistuje žádná technická možnost, jak zjistit, že na bankomat či pokladní terminál bylo nasazeno skimmovací zařízení nebo použita padělaná platební karta k výběru finanční částky. Nasazení skimmovacího zařízení lze zjistit pouze vizuálně, tedy např. pokud si občan všimne něčeho nezvyklého na bankomatu a tuto skutečnost oznámí [66]bance nebo policii. Občan zjišťuje fakt, že byla data z platební karty naskimmována, často až následně, většinou s větším časovým odstupem, a to jen proto, že na výpisu z účtu zjistí neoprávněně odčerpanou finanční částku a tuto skutečnost u vydávající banky reklamuje.

A pokud na bankomatu není nainstalována videokamera nebo je špatně nastavena, je zde další příčina ztíženého prověřování a odhalování pachatelů. Je pravdou, že se platební asociace, zejména VISA a MASTERCARD, snaží o prohloubení spolupráce s EUROPOLem a INTERPOLem a apelují na úzkou spolupráci bankovního sektoru se specializovanými policejními útvary jednotlivých zemí, avšak jednotlivé bankovní subjekty nadále v této oblasti postupují individuálně, čemuž se ani nelze divit, neboť se jedná o soukromoprávní, samostatně výdělečné prvky bankovního sektoru. Je zde sice vidět určité snahy o spolupráci, např. vytvořením Sdružení pro[67] bankovní karty České republiky a jeho Bezpečnostního výboru. Obdobně je tomu i ve Slovenské republice. Dochází k přímé komunikaci jednotlivých bank v rámci České republiky, ale i v rámci Evropské unie.

Jak vyplývá ze statutu Sdružení pro bankovní karty umístěného na jeho webových stránkách
(http://www.bankovnikarty.cz/web_sbk/czech/menu/o_sbk_cz.htm)

„ ...Sdružení pro bankovní karty je zájmovým sdružením právnických osob - bank příp. i jiných organizací, jejichž zájmem je rozvoj platebních karet v České republice a koordinace prací, souvisejících s tímto rozvojem. V zájmu svých členů jedná s tuzemskými i mezinárodními organizacemi z oblasti platebních karet. Sdružení pro bankovní karty bylo zaregistrováno u Obvodního úřadu Praha 1, dne 14.9.1992, podle § 201 i, odst. 2, zák. č. 47/92Sb pod č.j. 22/92…

Sdružení, které již od počátku svého vzniku kladlo velký důraz na zajištění bezpečnosti platebních karet v tuzemsku, je významným partnerem pro Policii ČR a bezpečnostní

[66] Zákon č. 21/1992 Sb., *o bankách*
[67] Zákon České národní rady č. 6/1993 Sb., o *České národní bance* ve znění následně vydaných novel

útvary platebních systémů. K tomu účelu byl ustaven "Bezpečnostní výbor SBK" jehož činnost významně *přispívá k odborné osvětě, snižování rizik i skutečných finančních ztrát z podvodů a kompletaci důkazních materiálů pro policejní šetření i soudní řízení. Od roku 1993 pravidelně organizuje setkání expertů v této oblasti ve spolupráci s mezinárodními platebními systémy MasterCard Europe , VISA EU, American Express a Diners Club. Na základě návrhu Bezpečnostního výboru byla dohodnuta a podepsána "Smlouva o společném postupu bank v oblasti akceptace platebních karet u obchodních partnerů", řešící základní pravidla pro omezení rizik podvodů v této oblasti.*

Činnost BV SBK významně přispěla k udržení kontroly nad vývojem rizika v polovině 90. let a k radikálnímu snížení úrovně podvodů s platebními kartami v ČR v letech 2000 až 2005 ….",

Jak vyplývá ze statutu Sdružení pro bankovní karty umístěného na jeho webových stránkách, je zřejmé, že pokud na úseku[68] padělaných platebních karet nebude na smluvním základě vytvořen obdobný mezinárodní, resp. národní systém jako u padělaných bankovek a mincí (národní centrální banky), bude tato oblast nadále problematická.

5.4.3.7 Analýza získaných poznatků

Jestliže se vrátíme zhruba do března 2007, tak v této době bylo zjištěno v České republice opravdu masivní nasazování skimmovacích zařízení na bankomaty zejména ve Středočeském, Východočeském, Severočeském kraji a na území hlavního města Prahy a to již od počátku[69] roku 2007. Bylo možné důvodně předpokládat, že této trestné činnosti se dopouští organizovaná skupina pachatelů. V téže době byl zjištěn výskyt a nasazení stejného skimmovacího zařízení v příhraniční oblasti Polska . Současně v týdenním odstupu od získání dat byl registrován výskyt padělků platebních karet s těmito daty, a to při výběrech finančních částek na bankomatech v České republice, ale i v Rumunsku, Slovensku a Maďarsku.

Protože bylo z časů nasazení skimmovacích zařízení i výběrů peněz na bankomatech zřejmé, že organizovaná skupina se dále dělí na podskupiny a takto se pohybuje, resp. může pohybovat prakticky po celé České republice, bylo rozhodnuto ze získaných poznatků zpracovat prvotní informaci a rozeslat ji cestou policejního prezidia všem

[68] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (*zákon o platebním styku*) ve znění zákona č. 257/2004Sb.
[69] HRADECKÝ, M.*Platební prostředky jejich ochrana a padělání.*Praha 2008.ISBN 80-7312-055-0

krajským správám v České republice. Cílem bylo informovat dotčené kraje a preventivně i ostatní o novém způsobu trestné činnosti na úseku padělání platebních prostředků a současně požádat o úzkou spolupráci jak s odborem padělání ÚOOZ, tak i s jeho expoziturami v krajích. Dále bylo potřeba zaměřit pozornost výkonných útvarů policie v rámci své denní pracovní činnosti jak na pachatele, tak na bankomaty, ale též na urychlené předávání jakýchkoliv relevantních poznatků prostřednictvím operačních středisek na dosahový telefon odboru padělání ÚOOZ. Neméně důležité bylo zajistit správný postup v případě zjištění skimmovacího zařízení (např. na místo nevysílat uniformované policisty v autech v barvách policie, ale pracovníky kriminální policie atd.).

Je pravdou, že nebylo zcela doceněno, že v rámci České republiky kromě Policie ČR existují ještě různé městské policie, příp. obecní policie. Bohužel tyto existují každá zcela samostatně a nemají žádný centrální zastřešující orgán. Proto nebylo možné tento druh policie informovat, pouze ve vytipovaných místech v omezeném počtu byla osobním jednáním navázána spolupráce a to zejména tam, kde obecní policie vlastní městský kamerový systém. Tento nedostatek se také projevil negativně v Teplicích, kde pracovník městské policie uviděl na kamerovém systému tři muže, jak blíže nedefinovaným způsobem s něčím podezřele na bankomatu manipulují, a iniciativně na místo poslal městské strážníky, kteří všechny tři zadrželi a předali OOP v Teplicích. Protože muži (rumunské národnosti) veškerou trestnou činnost popřeli (zařízení – tedy dřevěnou lištu bez další elektroniky údajně našli a jen tak si ji zkoušeli) a prověřením zejména otisků prstů v evidenci na Kriminalistickém ústavu nebyla zjištěna shoda s již dříve zajištěnými otisky ani nebyly zajištěny žádné jiné důkazy, bylo nutné všechny v zákonné lhůtě propustit na svobodu. Následně za tři měsíce byl zjištěn jejich výskyt na kamerovém systému na bankomatech v Praze při výběrech peněz na padělané platební karty, ovšem již se nepodařilo tyto pachatele v České republice zadržet.

Pachatelé při zkoušení funkčnosti skimmovacího zařízení a dále i pro oddělování získaných dat používají tzv. testovací karty (číslo začínalo 308…., 700….., 708…… a nejednalo se o platební, nýbrž klubové karty) bylo ve spolupráci s bankovním sektorem zajištěno u servisních subjektů bank trvalé monitorování výskytu těchto testovacích karet na bankomatech v rámci celé České republiky. Bylo zjištěno, že jako testovací karty používají pachatelé i pravé platební karty vystavené na své vlastní jméno bankami v Rumunsku i v České republice. Tyto platební karty si nechávali vystavit k založenému účtu na max. 100,-EURO s tím, že tuto částku často vyčerpali, karty jim byly na

bankomatech zadržovány a následně vydávány a dle poznatků Europolu byly také takovéto účty používány k tzv. „praní peněz“ získaných výběry z bankomatů na padělky platebních karet.

Je pravdou, že ne u všech krajských správ se tato analýza získaných poznatků opatření setkalo s kladnou odezvou. Na druhou stranu velice dobrá spolupráce byla s pracovníky odboru hospodářské kriminality správy Středočeského kraje a zejména s Okresním ředitelstvím Policie ČR v Liberci, kde se také následně potvrdilo, že zde opravdu pachatelé v počtu cca deseti osob byli na dvou místech ubytováni.

Kromě skimmování platebních karet se tito pachatelé zabývali v České republice nákupem motorových vozidel a jejich transportem do Rumunska. I díky tomuto poznatku se následně podařilo v podstatě celou skupinu ustanovit (v jednom případě měli tři pachatelé malou dopravní nehodu a pokusili se utéct a v druhém pachatelům někdo ukradl vozidlo a ti případ oznámili policii).

I když se nepodařilo zadržet pachatele a to z různých subjektivních i objektivních důvodů, přesto lze vykonanou činnost hodnotit pozitivně. Vždy však existovalo určité časové prodlení od doby nahlášení výskytu testovacích karet na konkrétním bankomatu a to přesto, že pro prvotní zajištění místa byla požadována spolupráce s nejbližším okresním ředitelstvím. Na druhou stranu se podařilo zajistit tři skimmovací zařízení i se získanými daty a bankovní sektor mohl provést potřebná opatření k zablokování všech dotčených platebních karet. Nakonec bylo zjištěno, a to jak prováděným šetřením, tak i z monitoringu testovacích karet, že pachatelé se začátkem července 2007 urychleně přes Rumunsko a SRN přemístili do Francie a Itálie.

5.4.3.8 Způsob použití skimmovacího zařízení

Z hlediska použitého skimmovacího zařízení jednotlivými pachateli bylo nejprve v Praze na základě zajištěných třech zbytků skimmovacího zařízení pracovníky odboru hospodářské kriminality správy hlavního města Prahy počátkem roku 2007 zjištěno používání nástavce na vstupní štěrbinu pro platební kartu (se zařízením na sejmutí dat z magnetického proužku platební karty) a k zjištění kódu PIN byl používán mobilní telefon (zřejmě pomocí videokamery v telefonu), který byl umístěn ve speciálním nástavci.

Výše uváděná skupina pachatelů rumunské a moldavské národnosti používala od března 2007 na získávání dat z platební karty různé nástavce na vstupní štěrbinu pro platební kartu (dle typu bankomatu) a pro získávání kódu PIN používali celou falešnou spodní desku s vlastní klávesnicí a speciálním zařízením na záznam dle zmáčknutého tlačítka.

V dalších případech ke konci roku 2007 se nepodařilo zjistit použitý typ skimmovacího zařízení, ale pravděpodobně minimálně jedna skupina rovněž na záznam kódu PIN používala mobilní telefon ve speciálním nástavci na bankomatu.

5.4.3.9 Pozitivní faktory použití při prověřování skimmingu

1) monitoring tzv. testovacích karet ze strany servisních složek pracujících za úplatu nebo ve prospěch bankovního sektoru – jednalo se o velmi úspěšnou metodu. Negativní však bylo to, že ji jednak provádělo více subjektů, nebyl resp. není pokryt celý bankovní sektor a hlavně bylo možné v tak širokém rozsahu ji použít jen jednou. V dalších případech se zřejmě pachatelé poučili a s testovacími kartami neprováděli již transakce, ale kartu pouze do bankomatu vsunuli a ihned transakci zrušili (což nelze on-line monitorovat)
2) ve spolupráci s bankovním sektorem se podařilo získat nejen čísla testovacích karet klubových, ale rovněž čísla platebních karet pachatelů a následně dle jejich výskytu, vytipovávat další používané karty
3) podařilo se získat v místech napadených bankomatů dle výpisů z buněk telefonní čísla mobilů v daném místě používaných a z nich vytipovat telefonní čísla zhruba deseti mobilních karet českého operátora (v číselné řadě po sobě jdoucích), které používali pachatelé
4) na základě osobního projednání byl v několika městech (např. Liberec, Turnov, Vrchlabí) využit existující městský kamerový systém a došlo ke spolupráci s městskou policií.Toto opatření však nešlo provést plošně, neboť ne všude je kamerový systém vybudován
5) vzhledem k nutnosti znaleckého prozkoumání zajištěných skimmovacích zařízení a získání okamžité informace o fungování tohoto zařízení byla na základě projednání s BLKA Mnichov navázána úzká spolupráce s tamějším znaleckým pracovištěm

5.4.4 Osvědčené faktory výše uváděné trestné činnosti

- vždy zjišťovat existenci jakéhokoliv dostupného kamerového sytému při nápadu této trestné činnosti a ihned zabezpečit na předmětnou dobu videozáznamy a zabránit jejich smazání (videokamery na bankomatu, v bankách, v hotelech, záznamy z městského kamerového systému, videokamer používaných na čerpacích stanicích, v obchodních centrech apod.)
- dopředu předpokládat možnost nalezení daktyloskopických a genetických stop a používat při manipulaci se zajištěným skimmovacím zařízením i padělanými platebními kartami plastické rukavice
- neprovádět zajišťování[70] stop na padělcích či skimmovacím zařízení na místě, ale následně na odborných pracovištích (OKTE, KÚ Praha)
- důsledně provádět šetření na místě, zejména na přilehlých parkovištích při výskytu podezřelých osob a vozidel do okruhu cca 150m od napadeného bankomatu, ale i ve stejném okruhu prověřit bankomaty na výskyt skimmovacího zařízení, vytěžovat nejen občany, ale i strážníky městské (obecní) policie
- v případě zajištění podezřelé osoby zajistit zejména její foto (operativně pořídit foto i dalších souvisejících osob), daktyloskopické otisky, provést důkladnou osobní prohlídku i prohlídku příp. používaného vozidla, zajistit veškerou nalezenou výpočetní techniku – zejména notebooky, fotoaparáty, mobilní telefony, PDA atd., včetně jakýchkoliv pamětí (přenosné Aiflash, karty z mobilů, fotoaparátů, videokamer apod.) a zadokumentovat používaná telefonní čísla a kódy PIN (pokud je osoba ochotná je sdělit) a čísla SIM karet a IMEI mobilů, zkontrolovat, a zajistit je, zda nalezené platební karty znějí na jméno podezřelé osoby, obdobně zkontrolovat (zajistit) nalezené věrnostní, klubové, telefonní a jakékoliv jiné karty s magnetickým proužkem na zadní straně, prověřit, zda na nalezených písemnostech není uváděn např. seznam kódů PIN (většinou seznam pořadových čísel a k nim připsané jedno až tři čtyřmístná čísla) apod.
- provádět fotodokumentaci zajištěných platebních, věrnostních, telefonních, klubových a jakýchkoliv jiných karet, včetně padělků karet
- je třeba si uvědomit, že padělky platebních karet mohou být vzhledem ke své velikosti ukryty kdekoliv ve vozidle a to i skrytě v různých dutinách (např.

[70] ZZ PP ČR č. 130/2007, kterým se upravuje *postup Policie ČR při plnění úkolů v trestním řízení* ve znění následně vydaných novel

v tunelu pod řadící pákou apod.), ale i např. v poloprázdné krabičce s cigaretami apod.

- v případě nálezu podezřelých platebních karet volat kdykoliv operační středisko ÚOOZ a žádat spolupráci odboru padělání ÚOOZ včetně potřebných konzultací
- při následném prověřování úzce spolupracovat s místní pobočkou banky jíž patří napadený bankomat (zejména žádat zajištění videozáznamů), dále stanoveným způsobem (dle zákona o policii nebo dle tr. řádu) vyžadovat u operátorů veškeré zjistitelné údaje na základě zajištěných IMEI mobilních telefonů, čísel SIM karet, příp. dle čísel mobilních telefonů
- dále vytěžit k případným. poznatkům zejména policisty z pořádkové služby, dopravní služby a městské policie apod., kteří se v rámci výkonu své služby mohli pohybovat v místě nápadu trestné činnosti

Je pochopitelné, že v současné době nelze poskytnout detailní návod, jak v případě nálezu skimmovacího zařízení, oznámení neoprávněného výběru na padělanou platební kartu či oznámení internetové (počítačové) kriminality postupovat. Částečně jsem se sice o to pokusil, ale vzhledem k rozsahu této trestné činnosti a k již uvedené operativnosti a konspirativnosti pachatelů je třeba klást důraz na zkušenosti a schopnosti policistů pracujících na daném případu a spoléhat se na ně. Odbor padělání ÚOOZ každoročně opakovaně zajišťuje a provádí proškolování policistů[71] zařazených na OHK jednotlivých krajských správ a v jednotlivých expoziturách ÚOOZ v krajích. Proškolování je nutné provádět a přenášet informace z krajského stupně i pro policisty zařazené na OHK okresních stupňů, ale i na dalších útvarech krajského a okresního stupně (dálniční, pořádková, dopravní, cizinecká policie, OOP atd.).

Na úplný závěr chci ještě informovat o požadavku EUROPOLU na úseku hlásné služby, který bude požadován od odboru padělání ÚOOZ za Českou republiku na úseku skimmování dat a padělání platebních karet, vč. výběrů finančních částek na padělané platební karty :

1) bude požadováno okamžité zasílání informací k jakémukoliv napadení bankomatu, bankovního konta, účtu či zneužití platební karty, a to do 24 hodin od zjištění

[71] ZPPP ČR č. 81/2003, kterým se upravuje *postup policie ČR při prověřování a vyšetřování trestných činů* v případech výskytu penězokazectví ve znění následně vydaných novel

2) k výše uvedenému budou požadovány následující údaje :

- druh (typ) bankomatu, datum, čas, adresa bankomatu (město a ulice), jméno banky, jaká platební karta byla použita (např. testovací, padělek), její číslo (číslo konta, účtu), foto podezřelé osoby z videozáznamu z kamery na bankomatu,k pachatelům bude třeba uvést jméno a příjmení, datum narození, foto, daktyloskopické otisky, zda je členem organizované skupiny, vozidlo, doklady, telefon (IMEI, výpisy volaných a přijatých hovorů, SMS, MMS, paměťová karta atd.).

Zatím není stanoven termín, odkdy budou výše uvedené údaje v rámci informačního systému EUROPOLEM požadovány. Policejní prezidium o této skutečnosti již bylo informováno v roce 2007 včetně faktu, že bude nutné provést odpovídající legislativní úpravy.

Je pochopitelné, že řadu požadovaných údajů bude nutné získávat od bankovního sektoru. Některé údaje lze v rámci teritoria (kraj, okres i obvod) získat v předstihu, jako např. druh bankomatu, jeho adresu nebo majitele[72] (banka) bankomatu. Problém však bude s fotografiemi podezřelých osob a to jednak proto, že ne všechny bankomaty jsou osazeny kamerovým systémem, ale hlavně proto, že u řady bank tuto službu zajišťuje další subjekt, často za úplatu a hlavně v neúměrně dlouhém časovém úseku. Tato oblast bude tudíž vyžadovat ze strany bank zejména organizační úpravy stávajícího systému a hlavně zrychlení zhotovení a předávání fotografií z videozáznamů policii. Dílčí problém může vzniknout při zjištění čísla použité karty, ale zde rovněž zřejmě půjde pouze o dodržení stanoveného časového intervalu.

Ze strany policie by při důsledném a řádném postupu neměly být problémy se zjišťováním informací o pachateli, příp. o jím použitém vozidle, neboť se jedná o běžný a zažitý postup a to včetně fotografování a daktyloskopování. Problém však může nastat u mobilů (PDA apod.) a to v případě, že místně příslušné OKTE (KÚ Praha) nebude vybaveno příslušnou technologií[73] včetně personálního zabezpečení, anebo pachatel před zadržením vypne mobilní telefon nebo zcela prozaicky se mobil sám vypne z důvodu nedostatečné kapacity akubaterie a pachatel odmítne sdělit blokovací kód a přístupový

[72] Zákon České národní rady č. 6/1993 Sb., o České národní bance ve znění následně vydaných novel
[73] Vyhláška České národní banky č. 523/2006 Sb., o podmínkách, za kterých lze reprodukovat bankovky, mince, šeky, cenné papíry a platební karty a vyrábět předměty, které je úpravou napodobují

kód mobilu. Další otázkou je, zda příslušná pracoviště OKTE (KÚ Praha) budou z kapacitních důvodů schopna zpracovat informace z mobilu, paměťové karty příp. dalších zařízení k úschově dat, neboť v současné době i v případě, že se nejedná o odborné vyjádření a policejní orgán žádá o tzv. úkon, je termín dodání řádově v měsících.

5.4.5 Výzkum uskutečněných zadržených skimmovacích zařízení

Pod obsah slov skimming platebních karet lze v současné době zahrnout několik způsobů páchání trestné činnosti jednotlivými pachateli, resp. organizovanými skupinami pachatelů, přičemž trestné činy mohou být páchány samostatně, společně nebo různě kombinovány. Následně uváděné způsoby získávání dat a kódů PIN nejsou v žádném případě taxativní, neboť pachatelé neustále vymýšlejí nové a nové způsoby trestné činnosti.

5.4.5.1 Magnetický proužek platební karty a kód PIN

Prvotní je získání dat z magnetického proužku platební karty a kódu PIN :

1) Nejvíce rozšířeno je získání dat z platebních karet prostřednictvím hackerů, kdy, hackři získávají velké množství dat z počítačů firem zabývajících se výrobou platebních karet, příp. napadením počítačů bankovního sektoru a to zejména v USA, Velké Británii, Irsku apod. Tímto způsobem byla již získána data z magnetických proužků platebních karet v řádech milionů kusů s tím, že následně se podařilo pachatelům rozkódovat PIN kód.
2) Druhým nejvíce rozšířeným způsobem je získávání dat z magnetických proužků platebních karet prostřednictvím speciálně vyrobených nástavců na štěrbiny pro vstup platební karty do bankomatu a pomocí dalších zařízení je získáván kód PIN.
3) Dalším způsobem získávání dat jsou různé způsoby phishingu, pharmingu apod., kdy pomocí podvodných mailů či celých webových stránek jsou uživatelé internetového bankovnictví žádáni z různých důvodů o sdělení čísel platebních karet, kódů PIN, čísel účtů, hesel apod.
4) Posledním zatím zjištěným způsobem je získávání dat z magnetického proužku platební karty a pokud je zadáván, tak i získání kódu PIN prostřednictvím upravených pokladních terminálů v hotelech, na čerpacích stanicích,

v obchodních řetězcích apod. Pachatelé je utajeně vymění za originální a následně, např. po měsíci, je odcizí.

Z hlediska ČR je nejvíce rozšířeným způsobem získání dat z magnetického proužku platební karty a zadávaného kódu PIN pomocí různých nástavců, jak je výše uvedeno pod bodem 2).

5.4.5.2 Zneužití padělků prostřednictvím internetového bankovnictví

1) Původně byly vyráběny kompletní padělky platebních karet, ale velice brzo pachatelé zjistili, že nejjednodušším a nejlevnějším způsobem je nahrání získaných dat na magnetický proužek [74]jakékoliv normalizované karty s magnetickým proužkem. Poté kartu použijí k výběrům finančních částek na bankomatech.

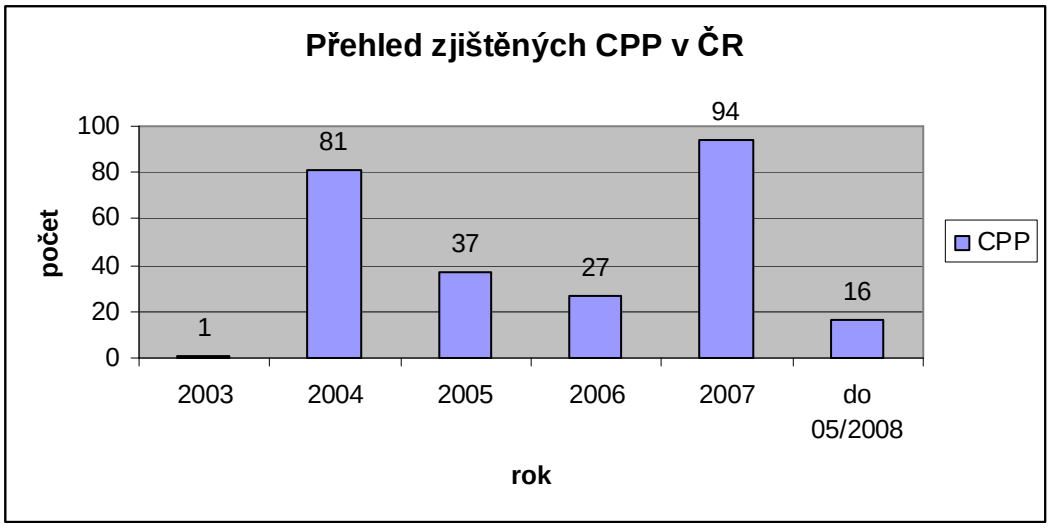
2) Druhým způsobem je zasílání kopií padělků platebních karet hotelům, obchodům a dalším subjektům za účelem nákupu zboží, objednání služeb či přeposlání tzv. ušetřených peněz na účet uvedený pachateli .

3) Posledním zatím zjištěným způsobem použití odcizených dat, a to velmi rozšířeným, je zneužití možností bezhotovostního platebního styku prostřednictvím internetu zasláním odcizených dat hotelům, obchodům, internetovým obchodům a dalším subjektům rovněž za účelem nákupu zboží, objednání služeb či přeposlání tzv. ušetřených peněz na účet uvedený pachateli nebo zneužití dat při nákupech v internetových obchodech, burzách či inzerci apod.

V ČR je nejvíce rozšířeným způsobem používání padělků platebních karet v bankomatech a zneužívání možností bezhotovostního platebního finančnictví přes internet. Byl např. i zjištěn případ vypůjčení a nevrácení vozidla z autopůjčovny, přičemž finanční částka za půjčení vozidla byla hrazena z padělané platební karty. Data z platebních karet a kódy PIN jsou často mezi pachateli distribuovány prostřednictvím internetu nebo pomocí zašifrovaného speciálního programu.

[74] ŠÁMAL ,P.*Podnikání a ekonomická kriminalita v České republice* . 1.vyd. - Praha: C. H. Beck, 2001 - xxv, 776 s. ISBN 80-7179-493-7

Vzhledem k tomu, že výše uvedená trestná činnost je značně latentní a v bankovním sektoru (jedná se o soukromoprávní sektor se snahou bagatelizovat vzniklé škody) neexistuje žádná komplexní evidence případů nasazení skimmovacích zařízení, natož případů výběrů peněz na padělané[75] platební karty, resp. případů použití nezákonně získaných dat z platebních karet, lze pouze na základě dílčích podkladů některých bank v ČR (počty v letech 2003-2006) a odboru padělání – Národní centrála proti penězokazectví ÚOOZ SKPV P ČR (počty v letech 2007 a 2008) uvést přibližné počty případů nasazení skimmovacích zařízení na bankomatech v ČR za poslední období (přičemž uvedené počty CPP v následující tabulce jsou dle našeho názoru přibližné a značně podhodnocené) :



Graf 3 - Zjištěné skimmovací zařízení
[zdroj] 20.

Poznámka: zkratkou CPP označuje bankovní sektor nasazené a zjištěné skimmovací zařízení na bankomatu, počty CPP získány z počtů dnů ve kterých různou dobu a v různých hodinách bylo na bankomatu nasazeno skimmovací zařízení.

Dle dostupných informací bylo od roku 2006 dosud prokazatelně zajištěno v ČR celkem 9ks skimmovacích zařízení, které mohla policie prozkoumat a vidět. Přirozeně byla zajištěna i další kompletní i částečná (většinou poškozená) skimmovací zařízení bankovním sektorem, o kterých se policie dozvěděla následně a pouze dle popisu, nebo vůbec.

[75] SADOVSKÝ, D.: *Odhalování trestné činnosti na úseku platebních karet*. Diplomová práce, PA ČR, Praha, 2003

5.4.6 Výzkum zneužití platebních karet v ČR

Ze zadržených skimmovacích zařízení, které lze prokazatelně alespoň částečně popsat se jedná o následující :

a) rok 2006 – bankomat ČS v Praze - 1, Mostecká ul. – kvalitně zpracovaný a oboustrannou lepicí páskou přilepený falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat a konektor na připojení k PC) a pro výdej potvrzenek. Na originální klávesnici přilepena falešná klávesnice (výše asi 1cm) s elektronikou na záznam zadávaného kódu PIN (propojené jednotlivé klávesy s mikrospínači, baterie, čip na ukládání dat a konektor na připojení k PC).

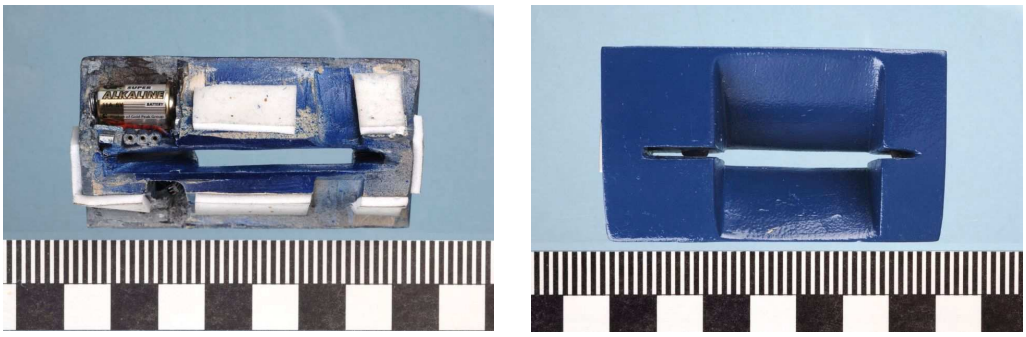
Obrázek 3 – Bankomat, falešný nástavec

[zdroj] 16.

b) rok 2007 - bankomat GEMB v Praze - 1, Opletalova ul. – zadržen pouze falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat a konektor na připojení k PC).

Obrázek 4 – Nástavec s vloženou elektronikou
[zdroj] 16.

c) rok 2007 – bankomat E-Bank v Praze - 1, Spálená ul. – zadržen pouze falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat a konektor na připojení k PC).



Obrázek 5 – Snímač dat z magnetického proužku
[zdroj] 16.

d) rok 2007 – bankomat ČS v Praze - 1, Kaprova ul. – falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat) a nástavec s mobilním telefonem na snímání zadávaného kódu PIN přilepený nad originální klávesnici na bankomat.

Obrázek 6 – Mobilní telefon na snímání kódu

[zdroj] 16.

e) rok 2007 – bankomat ČS v Mladé Boleslavi – falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat a konektor na připojení k PC) a pro výdej potvrzenek. Celý spodní panel bankomatu s originální klávesnicí překryt falešným panelem s falešnou klávesnicí s elektronikou na záznam zadávaného kódu PIN (propojené jednotlivé klávesy s mikrospínači, baterie, čip na ukládání dat a konektor na připojení k PC).

Obrázek 7 – Falešný nástavec s klávesnicí

[zdroj] 16.

f) rok 2007 – bankomat ČS v Teplicích, Masarykova ul. – falešný nástavec překrývající celý prostor vpravo od monitoru bankomatu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat a konektor na připojení k PC). Celý spodní panel bankomatu s originální klávesnicí překryt falešným panelem s falešnou klávesnicí s elektronikou na záznam zadávaného kódu PIN (propojené jednotlivé klávesy s mikrospínači, baterie, čip na ukládání dat a konektor na připojení k PC).

Obrázek 8 – Falešná klávesnice s elektronikou

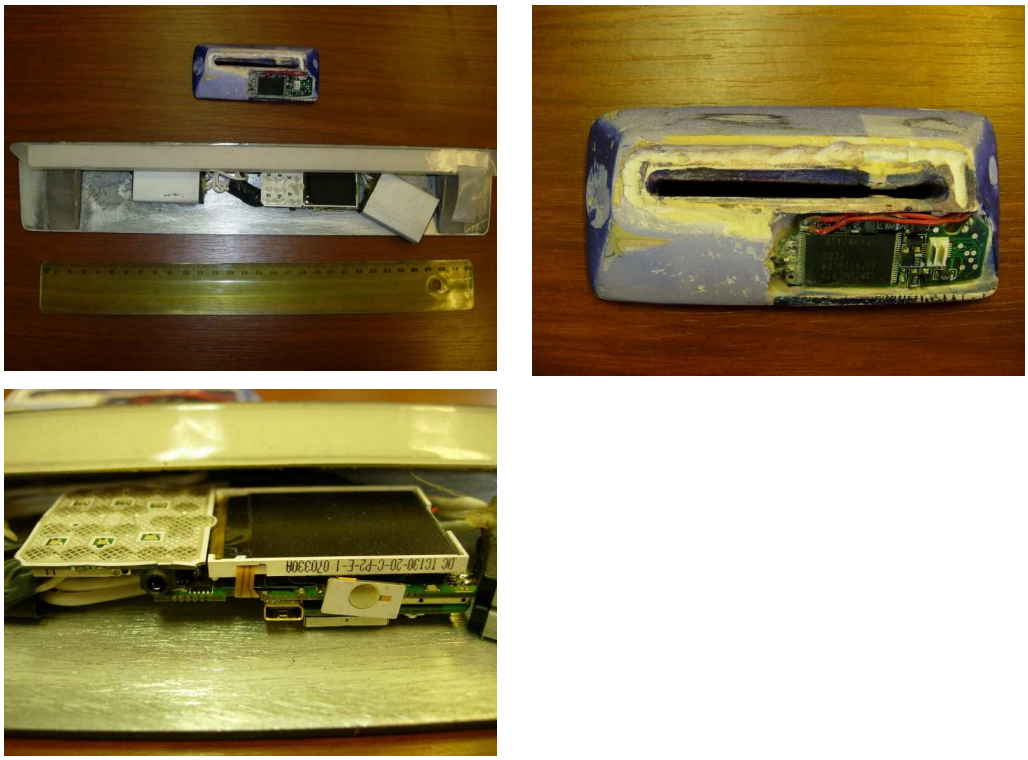
[zdroj] 16.

g) rok 2007 – bankomat GEMB v Mariánských Lázních, Hlavní ul. - falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat a konektor na připojení k PC). Celý spodní panel bankomatu s originální klávesnicí překryt falešným panelem s falešnou klávesnicí s elektronikou na záznam zadávaného kódu PIN (propojené jednotlivé klávesy s mikrospínači, baterie, čip na ukládání dat a konektor na připojení k PC).

Obrázek 9 – Propojení kláves s mikrospínači

[zdroj] 16.

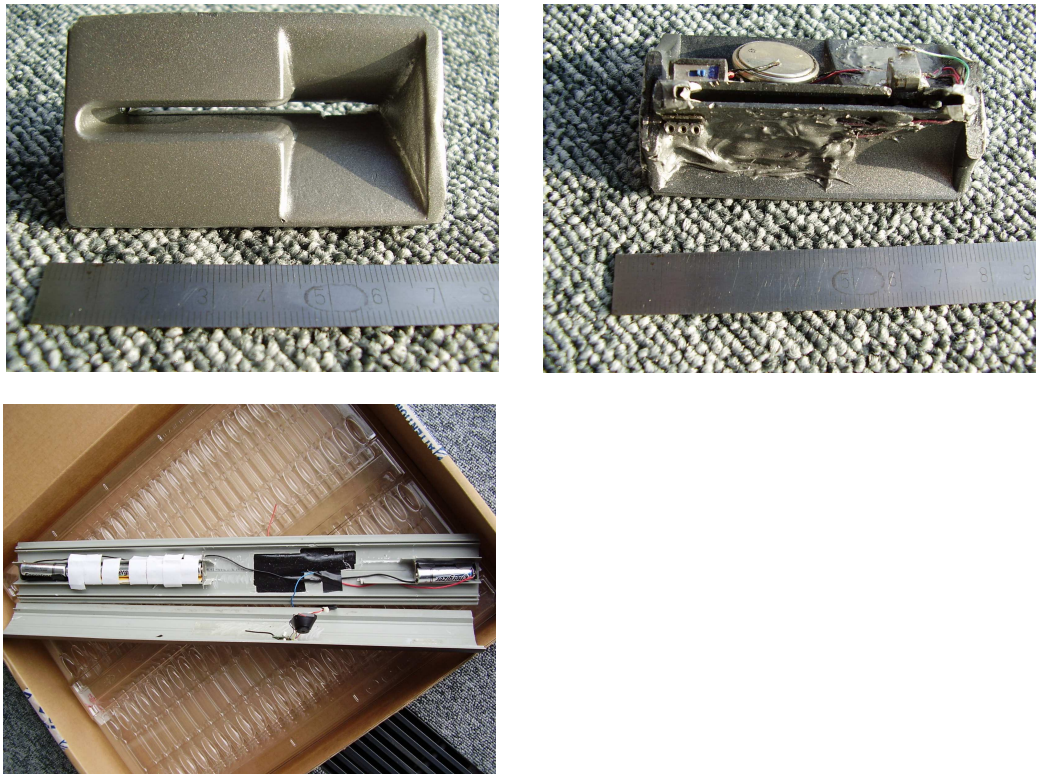
h) rok 2008 – bankomat Euronet v Praze - 1, Václavské nám. - falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie a elektronika na tištěném spoji, pravděpodobně z mobilu upravená na záznam či bezdrátový přenos dat) a nástavec s upraveným mobilním telefonem nebo PDA na snímání zadávaného kódu PIN přilepený nad originální klávesnici na bankomat (možnost záznamu dat nebo přímo bezdrátový přenos dat). Vzhledem k tomu, že na OHK hl. m. Prahy nebylo dosud zařízení předáno ke znaleckému zkoumání, není znám princip přenosu dat.



Obrázek 10 – Bezdrátový přenos dat

[zdroj] 16:

i) rok 2008 – bankomat ČSOB v Praze - 10, Černokostelecká ul. - falešný nástavec na vstupní štěrbinu pro platební kartu s vloženou elektronikou (snímač na data z magnetického proužku, baterie, čip na ukládání dat a konektor na připojení k PC) a nástavec s elektronikou na snímání zadávaného kódu PIN, přilepený nad originální klávesnici na bankomat (baterie, mikrokamera s anténou, dosud nezjištěné elektronické součásti).



Obrázek 11 – Přilepený falešný snímač
[zdroj] 16.

5.4.7 Zhodnocení výsledků výzkumu

Na základě výše uvedených způsobů získávání dat z magnetického proužku karty a kódu PIN lze konstatovat, že :

1) data jsou ukládána přímo do čipů ve skimmovacím zařízení a následně stahována do PC, doba nasazení na bankomatu od 1 hodiny do několika dnů dle kapacity použitých akubaterií nebo baterií

2) data jsou prostřednictvím mobilů, PDA či jejich částí (spojení wifi, bluetoth, sms) nebo jiného bezdrátového spojení přenášena on-line do PC nebo mobilu (umístěné dle dosahu použitého bezdrátového spojení, např. v zaparkovaném vozidle, v restauraci apod.), doba nasazení opět dle kapacity zvolených baterií

3) kombinace výše uvedených dvou způsobů

Podle teritoriálního hlediska je zjišťováno největší nasazování skimmovacích zařízení na bankomatech a obdobně i následné výběry peněz na padělky platebních karet .
V případě nasazení skimmovacího zařízení na bankomat použijí pachatelé získaná data k výrobě padělků platebních karet a následným výběrům peněz buď bezprostředně po získání dat v ČR, nebo bezprostředně zašlou data prostřednictvím internetu kamkoliv na světě, převážně do země původu a zde často i do 24 hodin již dochází k výběrům peněz na bankomatech, anebo si data uschovají a použijí po uplynutí delšího časového období (např. bylo zjištěno použití až po cca 1,5roku od naskimmování) opět kdekoliv ve světě včetně ČR. V řadě případů jedna organizovaná skupina získává data, příp. část skupiny ihned vyrábí padělky a vybírá peníze, nebo jiná organizovaná skupina přebírá data a vyrábí padělky a další členové pak provádí výběry. Jednotlivé skupiny se přemísťují operativně dle vlastní potřeby v rámci celé Evropy a v řadě případů i světa.

Z hlediska skimmování dat na pokladních terminálech, které jsou napojeny do elektrické sítě, ponechávají pachatelé skimmovací zařízení na místě až jeden měsíc. V ČR byly zjištěny pouze poznatky[76] k pachatelům ukrajinské národnosti, kteří se neúspěšně pokoušeli získat osobu, která by vyměnila upravený pokladní terminál za originální, resp. by umožnila použití padělaných karet. Dle informací Europolu byl tento způsob získávání

[76] Institut ministerstva spravedlnosti pro další vzdělávání soudců a státních zástupců: *Trestná činnost v bankovním sektoru*, 2. vyd. - Praha1997.187 s. ISBN 80-7256-482-3

dat v zahraničí již registrován (výměna terminálu byla provedena např. pomocí falešných servisních techniků nebo skrytým vloupáním do objektu apod.). Obdobně byl ve Francii již zaregistrován případ naskimmování dat z čipu umístěného na platební kartě a následné nahrání těchto dat na magnetický proužek padělku i nahrání dat na jinou čipovou kartu. Její použití dle dostupných informací zatím nebylo zjištěno.

Podle národnostního hlediska se na této trestné činnosti v roce 2007 nejvíce podílely osoby rumunské a moldavské národnosti. V prvním pololetí roku 2008 se podíl osob rumunské a moldavské národnosti na této trestné činnosti částečně snížil, ale dost razantně se zvýšil podíl občanů bulharské národnosti.

Co se týká způsobu provádění skimmování dat, jedná se o organizované skupiny osob znalé potřebné konspirace, které jsou značně opatrné, a jedná se převážně o osoby vždy z jednoho místa původu, resp. pobytu. Ke své činnosti ve velké míře využívají osob stejné národnosti, které v ČR mají povolení k trvalému pobytu za účelem sloučení rodiny, léčení apod. Skupiny osob rumunské národnosti v roce 2007 byly až desetičlenné, přijížděly do ČR na dobu až jednoho měsíce a kromě této trestné činnosti se zabývaly nákupem a dovozem ojetých vozidel do Rumunska. Po naskimmování potřebných dat na místě vyráběli padělky karet a ihned vybírali peníze, přičemž zřejmě internetem odesílali data do Rumunska, kde rovněž docházelo k výběrům peněz na padělky karet. V řadě případů používají tyto osoby falešné osobní doklady. Skupiny osob bulharské národnosti přijíždí v menším počtu, ale opakovaně v intervalu 7 až 14 dní, rovněž používají falešné osobní doklady, nebo mění identitu i formou soudní změny jména. Zde dochází ve větší míře k výběrům peněz na padělky v zahraničí, zejména v Bulharsku. V rámci aktuálně rozpracovaného případu bylo např. zjištěno, že jedna osoba bulharské národnosti přivezla do ČR opakovaně nezávisle na sobě další osoby,které byly v ČR zatčeny. Nadále v této činnosti pokračuje a dokonce vlastní vozidlo, které je řádně evidováno a má příslušné doklady a registrační značku jak v ČR, tak v Bulharsku (pod jedním a týmž číslem VIN).

Negativně se zde projevuje vstup Rumunska a Bulharska do EU a z toho vyplývající bezvízový styk, dále i vstup ČR do schengenského prostoru a následného ukončení provozu systému LOOK na hraničních přechodech apod. Na druhou stranu je třeba pozitivně hodnotit činnost Europolu, zejména na úseku činnosti pracovního týmu AWF TERMINAL, a to v oblasti sběru dat a jejich analýz, včetně předávání informací v rámci členských zemí Europolu. Podstatně se zlepšila výměna informací s Bulharskem i Rumunskem po vyslání českého styčného důstojníka pro Bulharsko, Rumunsko a Moldávii, a to zejména po navázání jeho osobních kontaktů s příslušnými policejními

orgány. Na základě navázaných osobních kontaktů je rovněž. dobrá spolupráce v Polsku a Slovensku.

Vzhledem k masivnímu nárůstu nasazování skimmovacích zařízení v ČR v roce 2007 začala Česká spořitelna iniciativně v polovině roku 2007 osazovat vlastní bankomaty tzv. antiskimmovacím zařízením. Jednalo se o nástavec na vstupní štěrbinu pro platební kartu z tvrzeného průhledného plastu zelené barvy (slangově nazývaný „zelený zobák“) připevněného k bankomatu čtyřmi šrouby, díky němuž prakticky okamžitě přestali pachatelé napadat bankomaty ČS. Následně začaly stejným způsobem chránit bankomaty i další [77]banky. Teprve v roce 2008 pachatelé na bankomatu GEMB v Praze a Plzni tento antiskimmovací nástavec utrhli a nalepili na štěrbinu svůj vlastní s elektronikou na snímání dat z magnetického proužku.

Obdobně na jiný typ bankomatu užívaný převážně GEMB a ČSOB začaly tyto banky nasazovat antiskimmovací zařízení, rovněž na vstupní štěrbinu pro platební kartu. Toto antiskimmovací zařízení bylo však z úsporných důvodů vymyšleno značně nedokonale, proto nyní není možné zjistit, zda na bankomatu je originální antiskimmovací zařízení nebo skimmovací zařízení. Tohoto faktu i jednoduché montáže využili pachatelé, kteří bez problémů začali originální antiskimmovací zařízení upravovat, resp. doplňovat potřebnou elektronikou a vyměňovat za originální. Dle zjištěných informací pachatelé buď antiskimmovací zařízení z bankomatu odtrhnou a upraví, nebo v zahraničí přímo zakoupí a opět upraví.

Určit, jaký typ bankomatu je nejčastěji pachateli napadán, nelze, protože bankovní sektor používá různé typy bankomatů, resp. různé varianty základních typů, a to i u jedné banky. Navíc bankovní sektor tyto informace utajuje a nebylo dosud možné získat nejen přehled používaných typů bankomatů, ale ani celkový aktuální přehled používaných a zabudovaných bankomatů (označení, adresu umístění, příslušnost ke konkrétní bance). Obdobně jsme cestou Bezpečnostního výboru SBK požadovali opakovaně zapůjčení tzv. testovacích karet pro operativní činnost, avšak dosud jsme je na odbor padělání neobdrželi.

Z hlediska výše uvedených zařízení i získaných poznatků a informací lze konstatovat, že pachatelé si vytipovali určité typy bankomatů a na tyto pak začali vyrábět skimmovací zařízení (příslušné nástavce). Ze začátku si pravděpodobně dováželi kompletní zařízení,

[77] Institut ministerstva spravedlnosti pro další vzdělávání soudců a státních zástupců: *Trestná činnost na českém kapitálovém trhu*, 1 – vyd. Praha,1997. 115 s. . ISBN 80-71214-493-5

pak jen elektroniku a polotovary z plastů (tzv. kopyto), kovu a dřeva a následně tyto nástavce zřejmě vyráběli přímo na místě, resp. „doupravovali. „

K jejich výrobě nástavců lze zcela běžně v obchodech nakoupit laminovací soupravy, barvy, tmely, izolační i samolepicí oboustranné pásky apod. Obdobně dle znaleckého vyjádření odborného pracoviště BLKA Mnichov jsou v obchodech s elektronikou dostupně k zakoupení veškeré elektronické součástky (baterie z mobilů, kulaté akubaterie, klasické baterie, čipy, mikrokamery, zdířky, přepínače, tištěné spoje, spojovací materiál, části mobilů apod.).

Jak již bylo uvedeno, pachatelé buď získávají data z magnetického proužku platební karty a kód PIN zadávaný oprávněným držitelem platební karty nebo pomocí padělaných platebních karet vybírají finanční hotovost. Jedna z forem této [78]trestné činnosti probíhá prostřednictvím internetu a druhá prostřednictvím bankomatů, resp. pokladních terminálů. V některých případech používali pachatelé na vyzkoušení funkčnosti skimmovacího zařízení tzv. testovací karty (buď vlastní platební karty nebo různé vstupní a dobíjecí karty).

Ze strany Národní centrály proti penězokazectví ÚOOZ SKPV P ČR (dále jen odbor padělání) je situace v současné době bez ohledu na nedostatečné personální a materiální vybavení speciálním zařízením a software taková, že úseku této trestné činnosti páchané prostřednictvím internetu nelze proti pachatelům účinně zasahovat, jedinou možností je upozornit příp. předat získané poznatky oddělení počítačové kriminality Policejního prezidia ČR.

Obecně odbor padělání má v současné době omezené možnosti zasahovat proti pachatelům uvedené trestné činnosti, lze to pouze ve spolupráci s bankovním sektorem u forem trestné činnosti prováděné prostřednictvím bankomatů, resp. pokladních terminálů, a to ještě převážně až po zjištění trestné činnosti, kdy pachatelé jsou již dávno mimo území ČR. Existuje sice spolupráce s Bezpečnostním výborem SBK pro ČR (SBK pro ČR však je zájmovým sdružením právnických osob-bank, příp. jiných organizací a ne všechny banky jsou jeho členem), ale vzhledem ke statutu tohoto sdružení a dále faktu, že banky jsou soukromé subjekty, těžko lze vytvářet nějaká systémová opatření, natož vyžadovat bezprostřední informace a poznatky. Získané informace a poznatky převážně vyplývají z osobních kontaktů zástupců odboru padělání se zástupci bankovního sektoru. Činnosti prováděné bankovním sektorem jsou totiž poměřovány především finančními

[78] SMEJKAL, V. *Právo informačních a telekomunikačních systémů.* Praha : C. H. Beck, 2004. xxx, 770 s. ISBN 80-7179-765-0

hledisky, názory jednotlivých právních oddělení bank na bankovní tajemství, vzájemnou malou snahou bank informovat se navzájem o vzniklých problémech, malou vnitřní spoluprácí příslušných pracovišť uvnitř bank, výkonem servisních služeb pro banky ze strany dalších soukromých subjektů (např. na úseku provozu bankomatů, videozáznamů, hardware[79] a software atd.).

V této souvislosti je třeba uvést, že podobná situace, spíše ještě horší než u platebních karet, je i na úseku padělaných šeků, a to jak u bankovního sektoru, tak i u policie, kde se policie stává pouhým zapisovatelem a evidenčním článkem (zde je hlavní důvod v tom, že sice na území ČR jsou provedeny všechny potřebné úkony, ale tím vše skončí, protože pachatel se nachází v zahraničí a spolupráce např. s Nigerií nebo i Velkou Británií je téměř nulová).

Odbor padělání nabízí spolupráci a pomoc nejen prováděním metodických školení, ale i přímo při prošetřování i realizaci jednotlivých případů (např. v roce 2007 v rámci vlastní akce SKIMMING SEVER). Je však pravdou, že v rámci tohoto případu na území Prahy, Středočeského, Severočeského a Východočeského kraje byla sice velmi dobrá spolupráce s OŘ Policie Liberec, expoziturou ÚOOZ Teplice a jedním pracovníkem na úseku padělků z OHK Středočeského kraje, ale reakce některých krajských správ na rozeslané upozornění o novém způsobu páchání a odhalování trestné činnosti na úseku platebních karet byla mírně řečeno podivná. Lze uvést jeden příklad, kdy na vyžádání měl do doby příjezdu policistů z odboru padělání a expozitury Teplice v mimopracovní době v Teplicích hlídat a příp. provést šetření v okolí bankomatu se skimmovacím zařízením policista v civilu a v civilním autě – výsledek byl ten, že šikmo naproti bankomatu přes ulici stálo vozidlo v barvách policie s uniformovaným policistou. Obdobně některé správy byly dotčeny, že se odbor padělání sice cestou náměstka policejního prezidenta vůbec pokouší žádat kraje o informaci od jejich vlastních policistů o tomto způsobu trestné činnosti a hlavně žádostí o spolupráci v rámci případu.

V době prošetřování v rámci případu SKIMING SEVER byla situace následující. Protože bylo zjištěno operativní cestou používání testovacích karet (včetně vlastních platebních karet) pachateli, bylo u bankovního sektoru vyžádáno monitorování těchto

[79] HRADECKÝ, M. *Platební prostředky jejich ochrana a padělání.* Praha 2008. ISBN 80-7312-055-0

karet. Výskyt těchto karet byl ihned ze strany několika soukromých subjektů předáván telefonicky na určený mobil odboru padělání, který měl přidělený policista zařazený na úseku platebních karet a byl v podstatě až na výjimky bezplatně v trvalém dosahu cca 5měsíců a dle předaných informací je vyhodnocoval a dle potřeb operativně ve spolupráci s vedoucím odboru zabezpečoval výjezdy pracovníků odboru na místo, resp. zajišťoval do doby jejich příjezdu cestou operačních středisek nebo v Liberci přímo u určených pracovníků OHK zajištění místa a provádění operativních šetření. Vzhledem k tomu, že v rámci odboru padělání měli i další pracovníci k dispozici vozidlo v mimopracovní době, nebyl problém ihned na místo vyslat maximální počet policistů odboru. Nejednalo se však o trvalé systémové opatření, nyní již není k dispozici žádný mobil se SIM kartou, navíc pro příp. dosah odboru a dosahy v rámci ÚOOZ nejsou nyní řešeny dle problematik odborů. Obdobná situace byla ve spolupráci s teritoriálními útvary Policie ČR a městskou či obecní policií. Kde se podařilo předem navázat osobní kontakty, bylo možné u Policie ČR bez zdlouhavého vysvětlování požadovaných úkonů několika lidem ihned na místo vyslat již poučené pracovníky kriminální služby, nebo v případě městských (obecních) policií využívat jejich kamerového systému (problém však u této policie je , že neexistuje žádné centrální zastřešení).

V případě podezření na výskyt skimmovacího zařízení na bankomatu, které vyplývalo z oznámení použití testovací karty (opakovaně) na bankomatu, bylo jednak ověřováno, zda se na bankomatu opravdu vyskytuje skimmovací zařízení, pokud ano, bylo prováděno operativní šetření za účelem[80] zjištění podezřelých osob, vozidel apod. Preventivně byly prověřovány vytipované bankomaty na výskyt skimmovacího zařízení a podezřelých osob a vozidel v blízkém okolí v různou denní dobu a to i v mimopracovní době.

Dále bylo možné zajistit video z městského kamerového systému či z videokamer jiných subjektů, příp. zajistit monitoring pomocí kamerových systémů. Současně bylo ihned u bankovního sektoru vyžadováno totéž, pokud bankomat byl osazen videokamerou a byly vytěžovány tyto videozáznamy a srovnávány s videozáznamy dříve napadených bankomatů. Další možností v širším horizontu byla obdobná činnost při vytěžování monitoringu provedených transakcí na podezřelém bankomatu a zjišťování použitých telefonních čísel v různých místech napadených bankomatů a tipování použitých stejných mobilních čísel na různých místech dle výpisů z buněk.

[80] KUCHAŘ, M. Bezpečná síť.Jak zajistíte bezpečnost vaší sítě. 1. vyd. Praha: Grada Publishing, 1999. 92 s. ISBN 80-7169-886-5

5.4.8 Závěrečné zhodnocení zkoumané problematiky a jejího vývoje

5.4.8.1 Pozitivní faktory

1) on-line monitoring tzv. testovacích karet ze strany servisních složek pracujících za úplatu nebo ve prospěch bankovního sektoru a operativní předávání zjištěných informací odboru padělání – jednalo se o velmi úspěšnou metodu. Negativní však bylo to, že ji jednak provádělo více subjektů a nebyl, resp. není pokryt celý bankovní sektor
2) ve spolupráci s bankovním sektorem se podařilo získat nejen čísla testovacích karet – klubových, členských apod., ale rovněž čísla platebních karet pachatelů a následně dle jejich výskytu vytipovávat další používané karty
3) podařilo se získat v místech napadených bankomatů dle výpisů z buněk telefonní čísla mobilů v daném místě používaných a z nich vytipovat telefonní čísla zhruba deseti mobilních karet českého operátora (v číselné řadě po sobě jdoucích), které používali pachatelé
4) včasné získávání videozáznamů od bankovního sektoru z bankomatů a tipování pachatelů
5) na základě osobního projednání byl v několika městech (např. Liberec, Turnov, Vrchlabí) využit existující městský kamerový systém a spolupracováno s městskou policií, toto však nešlo provést plošně a ne všude je kamerový systém vybudován
6) vzhledem k nutnosti znaleckého prozkoumání zajištěných skimmovacích zařízení a získání okamžité informace o fungování tohoto zařízení na základě projednání s BLKA Mnichov velice dobře spolupracováno s tamějším znaleckým pracovištěm
7) velmi dobrá přímá osobní spolupráce s policejními orgány SRN (zejména BLKA Mnichov), Slovenska a Polska

5.4.8.2 Negativní faktory

Na straně bankovního sektoru

- nedostatečná technická i personální ochrana bankomatů proti skimmovacím zařízením, utajování informací o bankomatech, zabudovaných videokamerách všech odborů bank, malá vnitřní informovanost atd.
- neznalost používaných skimmovacích zařízení na bankomatech ze strany pracovníků bank, pracovníků servisních služeb, pracovníků bezpečnostních agentur atd.

- chybějící nebo špatně nastavené videokamery na bankomatech a ve vstupních prostorách před i uvnitř banky
- v počáteční a závěrečné fázi pozdní předávání poznatků odboru padělání při podezření na výskyt skimmovacích zařízení a o prováděných výběrech na padělané platební karty na bankomatech v ČR
- pozdní předávání videozáznamů a zejména zpracovaných fotografií z těchto videozáznamů policii, krátké a různé ukládací doby videozáznamů a různorodý nahrávací a přehrávací software, vč. nesouladu uváděného času na videozáznamech se skutečným časem
- neexistence centrální evidence a monitoringu na úseku padělání platebních karet z vnitrostátního i mezinárodního hlediska
- vzhledem k dlouhé době šetření (cca 5 měsíců) postupné opadávání zájmu o věc ze strany bankovního sektoru, a to zejména z hlediska finančního

5.4.8.3 Na straně policie

- neznalost policistů o tomto druhu trestné činnosti a nevěnování pozornosti podezřelým okolnostem při běžném výkonu služby
- nezjištění a nepředávání poznatků k této trestné činnosti ze strany pořádkové, dopravní policie a dalších výkonných policistů při běžném výkonu služby věcně a místně příslušným policistům zařazený na kriminální službě
- složité vysvětlování žádosti ad-hoc o spolupráci více subjektům (operační středisko, policisté ve výjezdu atd.), i když předem byly krajské správy informovány písemně o možnostech napadání bankomatů skimmovacím zařízením a o nutnosti spolupráce s odborem padělání
- neexistence evidence nápadu skimmovacích zařízení, padělků platebních karet, včetně fotografií podezřelých a pachatelů v IS [81]BANKA s propojením na obdobnou evidenci bankovního sektoru a možnosti doplňování o informace zasílané z Europolu a Interpolu
- chybějící materiálně-technické vybavení odboru padělání ÚOOZ a expozitur ÚOOZ pro operativní činnost v terénu na úseku padělání platebních karet, např. chybějící speciální techniky a software na čtení dat z magnetických proužků platebních karet (obdobně z čipů platebních karet) a notebooků, vč. oficiálních

[81] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (*zákon o platebním styku*) ve znění zákona č. 257/2004Sb

testovacích karet z bankovního sektoru s tím, že ještě horší situace je na krajském a okresním stupni

- neexistence speciálního software na srovnávání fotografií podezřelých osob (např. fotografie zhotovených z videozáznamů a fotografie z evidencí)
- nemožnost proniknutí policisty nebo informátora do organizovaných skupin pachatelů vzhledem k jejich složení (osoby jedné národnosti, osoby blízké – kamarádi apod.)
- chybějící policisté na úseku počítačové kriminality na krajském a okresním stupni, nedostatečné personální obsazení zejména OHK na krajských a okresních stupních zkušenými policisty, ne vždy fungující vzájemná spolupráce apod.
- nepřiměřeně dlouhé doby na KÚ Praha a OKTE při zkoumání zajištěných skimmovacích zařízení z hlediska odborných vyjádření či znaleckých posudků, nemožnost získání operativních informací z těchto pracovišť ohledně veškeré zajištěné výpočetní či mobilní techniky
- problémy s operativním získáváním datových i obrazových informací (osobní data, fotografie podezřelých a pachatelů, informace o nápadu a způsobu trestné činnosti), včetně kopií daktyloskopických karet cestou Europolu (Interpolu) od zahraničních policejních útvarů
- zrušení systému LOOK v rámci vstupu do schengenského prostoru na hraničních přechodech, včetně nedokonalosti tohoto systému v době jeho fungování a nutností nahradit jej dokonalejším systémem, zvážit možnost využití kamerových záznamů z mýtného systému apod.

5.4.8.4 Na straně ostatních subjektů

- neexistence městských kamerových systémů, krátké ukládací doby, nemožnost centrálního informování městských a obecních policií a vyžádání jejich spolupráce v daném teritoriu v případě potřeby
- volný pohyb osob bez vízové povinnosti v rámci Evropské unie (problém u pachatelů např. z Rumunska a Bulharska)
- poskytování ubytování cizincům bez odpovídající evidenční a hlásné služby ze strany ubytovatelů
- zneužívání azylové politiky České republiky (např. získávání trvalého pobytu za účelem sloučení rodiny, pobyt za účelem léčení)

V této souvislosti je třeba poukázat ještě na několik faktorů obecnějšího charakteru, které vyplynuly při odhalování a prověřování výše uváděné[82] trestné činnosti :

- vždy zjišťovat existenci jakéhokoliv dostupného kamerového sytému při nápadu této trestné činnosti a ihned zabezpečit na předmětnou dobu videozáznamy a zabránit jejich smazání (videokamery na bankomatu, v bankách, v hotelech, z městského kamerového systému, videokamer používaných na čerpacích stanicích, v obchodních centrech, soukromých objektech apod.)
- dopředu předpokládat možnost nalezení daktyloskopických a genetických stop a používat při manipulaci se zajištěným skimmovacím zařízením i padělanými platebními kartami plastické rukavice
- neprovádět zajišťování stop na padělcích či skimmovacím zařízení na místě, ale následně na odborných pracovištích (OKTE, KÚ Praha)
- důsledně provádět šetření na místě, zejména na přilehlých parkovištích a u výskytu podezřelých osob a vozidel do okruhu cca 150m od napadeného bankomatu, ve stejném okruhu prověřit bankomaty na výskyt skimmovacího zařízení, vytěžovat nejen občany, ale i strážníky městské (obecní) policie
- v případě zajištění podezřelé osoby zajistit zejména její foto (operativně pořídit foto i dalších souvisejících osob), daktyloskopické otisky, provést důkladnou osobní prohlídku i prohlídku příp. používaného vozidla, zajistit veškerou nalezenou výpočetní techniku – zejména notebooky, fotoaparáty, mobilní telefony, PDA atd., včetně jakýchkoliv pamětí (přenosné Aiflash, karty z mobilů, fotoaparátů, videokamer apod.) a zadokumentovat používaná telefonní čísla a kódy PIN (pokud je osoba ochotná je sdělit) a čísla SIM karet a IMEI mobilů, zkontrolovat (příp. zajistit), zda nalezené platební karty znějí na jméno podezřelé osoby, obdobně zkontrolovat (zajistit) nalezené věrnostní, klubové, telefonní a jakékoliv jiné karty s magnetickým proužkem na zadní straně (čipem), prověřit, zda na nalezených písemnostech není uváděn např. seznam kódů PIN (většinou seznam pořadových čísel a k nim připsané jedno až tři čtyřmístná čísla) apod.
- provádět fotodokumentaci zajištěných platebních, věrnostních, telefonních, klubových a jakýchkoliv jiných karet, vč. padělků karet

[82] ZPPP ČR č. 81/2003, kterým se upravuje *postup policie ČR při prověřování a vyšetřování trestných činů* v případech výskytu penězokazectví ve znění následně vydaných novel

- je třeba si uvědomit, že padělky platebních karet mohou být vzhledem ke své velikosti ukryty kdekoliv ve vozidle, a to i skrytě v různých dutinách (např. v tunelu pod řadící pákou apod.), ale i např. v poloprázdné krabičce s cigaretami apod.
- při následném prověřování úzce spolupracovat s místní pobočkou banky jíž patří napadený bankomat (zejména žádat zajištění videozáznamů), dále stanoveným způsobem (dle zákona o policii nebo dle tr.řádu) vyžadovat u operátorů veškeré zjistitelné údaje na základě zajištěných IMEI mobilních telefonů, čísel SIM karet, příp. dle čísel mobilních telefonů
- dále vytěžit k příp. poznatkům zejména policisty z pořádkové služby, dopravní služby a městské policie apod., kteří se v rámci výkonu své služby mohli pohybovat v místě nápadu trestné činnosti
- maximálně prohlubovat osobní spolupráci se zahraničními policejními útvary (osobní kontakty, styční důstojníci, pracovní stáže atd.)
- vzhledem k značnému nárůstu trestné činnosti na úseku platebních karet a mírnému poklesu počtu padělků bankovek přizpůsobit organizaci odboru padělání ÚOOZ této situaci (je nutné vzít v potaz i oblast padělání šeků), včetně zvážení buď vytvoření expozitur ÚOOZ pro Prahu a Středočeský kraj, resp. zvýšení tabulkových počtů odboru padělání
- v případě nálezu podezřelých platebních karet nebo v případě jakékoliv potřeby konzultace volat kdykoliv operační středisko ÚOOZ a žádat spolupráci odboru padělání ÚOOZ, resp. předat zjištěné informace

6 PŘÍNOSY DISERTAČNÍ PRÁCE

Přínos disertační práce je v naplnění jejích cílů a lze jej formulovat jak v rovině teoretické, tak i v rovině praktické. Vzhledem ke skutečnosti, že praxe nemůže existovat bez teorie, je třeba zdůraznit vzájemnou provázanost obou přínosů. Na základě jejich průniku je pak možné formulovat nové poznatky, které lze využít v pedagogickém procesu.

6.1 PŘÍNOSY PRO NOVÉ VĚDECKÉ POZNÁNÍ

Vzhledem k tomu, že v současné době není zpracování souhrnné problematiky rizik bezhotovostních plateb, výběru peněžních částek v hotovosti a dalších finančních transakcí pomocí platebních karet, potažmo disertační práce, v rovině nového vědeckého poznání spatřuji v provedení komplexní analýzy na českém kapitálovém trhu.Tím bylo prohloubeno současné vědecké poznání . Důraz byl kladen na zjištění všech hlavních bariér získávání padělání a napodobování platebních karet a informačních prostředků. Za tímto účelem byl proveden primární výzkum kvantitativního charakteru, který byl zaměřen na danou problematiku z pohledu českých uživatelů.

Za další přínosy pro nové vědecké poznání lze považovat:

- Systémové vymezení celého řetězce vztahů B2C (prodej podnikatele spotřebitelovi) s důrazem na rozšíření nového pojetí kyberprostoru plateb
- Vyjádření modelu řízení elektronického obchodování a řízení plateb v systému strategického řízení firem a to možnými moderními prostředky ekonomické kybernetiky
- Nové chápání integrovaného elektronického prostředí s naznačením moderních teoretických znalostních atributů bezpečných bezhotovostních plateb
- Příspěvek do systémového vymezení platebních aktivit kartami v rozvoji nové strategie boje s kyberzločinem u nových bezpečnostních složek státu
- Vyjádření informačního a komunikačního prostředí elektronického obchodu je dílčím příspěvkem v rozvoji nové oblasti Obchodního zpravodajství

Dalšími přínosy technického charakteru jsou:

- skimmování a jeho možnosti
- vývoj úrovně poznání v oblasti možného zneužívání platebních karet vydávaných různými eminenty

6.2 PŘÍNOSY PRO PRAXI

Za nejvýznamnější přínosy disertační práce pro praxi lze považovat stanovení předpokladů pro uskutečnění formulace rizik plynoucích ze zneužívání platebních karet v podmínkách českého kapitálového trhu, návrh postupu, jak by měli postupovat.
Mezi další přínosy pro praxi patří:

Systémové chápání integračních procesů v elektronickém prostředí zasahující všechny nové oblasti obchodování v globálním světě. Odtud bude také potřeba zpracovat nové metodické pomůcky pro bezpečné provozování elektronického obchodu a systému ochrany informací v bezhotovostním platebním styku.

Práce je příspěvkem pro další oblasti:

- navržení optimálního modelu ochrany platebních karet, včetně návrhu nových trendů v této oblasti, které povedou k významnému zvýšení jejich ochrany a spolehlivosti před zneužitím
- formulace rizik plynoucích ze zneužívání platebních karet a jejich zařazení do tříd nebezpečnosti
- návod opatření pro eminenty platebních karet
- uplatnění výsledků práce v oblasti kriminalistické prevence a praxe.

Provedený výzkum má bezprostřední vliv na vlastní strategii firmy.

6.3 PŘÍNOSY PRO PEDAGOGICKÝ PROCES

Předpokládá se, že výsledky disertační práce budou využity v pedagogickém procesu ve formě zpracování odborné literatury (případové studie, odborné publikace) určené studentům vysokých škol ekonomického zaměření i širší odborné veřejnosti.
Především to bude posílení předmětu Elektronický obchod pro Manažerskou informatiku v oblasti Elektronického bankovnictví, dále v předmětu Elektronické podnikání a dvou předmětech Elektronické bankovnictví a Krizový management elektronického bankovnictví.
Pro doktorandské studium při obohacení studia Teorie systémů a Znalostní management.

Získané poznatky by mohly zhodnotit a doplnit výuku v rámci speciálních kurzů a seminářů pro vybrané pracovníky policie zaměřené na tuto dnes poměrně rozsáhlou a nebezpečnou kriminální činnost.

7 NÁMĚTY K DALŠÍMU VÝZKUMU

V průběhu disertační práce byly objeveny další možnosti pro pokračování a rozšíření zkoumané oblasti, kterými bych se rád zabýval ve své budoucí výzkumné činnosti.

Náměty k dalšímu výzkumu lze v obecném pojetí formulovat v následujících bodech.

- pokračování v kvantitativním výzkumu respondentů, kteří v budoucnu na českém kapitálovém trhu a na základě získaných poznatků doplnění a rozšíření výsledků analýzy uskutečněné v České republice
- další výzkumné aktivity mohou směřovat do oblasti rozvoje znalostní gramotnosti Obchodního zpravodajství, rozvoje vhodného prostředí pro kyberprostor. Bezpečnostní strategie bankovního sektoru, pomoci při rozvoji výzkumných aktivit Bezpečnostní strategie elektronického obchodování pro potřeby PČR a Prevence kriminální činnosti v elektronickém obchodu

8 ZÁVĚR

Vznikají nové společnosti. Mnohé z nich zaniknou v prvních měsících svého života, jiné se prosadí rychlostí a stylem, který byl ještě před pěti lety nemyslitelný. Intelektuální hodnota firem začíná převažovat nad suchými čísly uvedenými v rozvaze a výsledovce. Jen tak lze vysvětlit obrovský růst cen akcií firem jen několik měsíců starých. Dnes se vsází na budoucnost. Je dobré si vzít poučení z nedávné historie. Kdo by si dovolil před 15 lety odhadnout, že klasické telefony budou mít velkého konkurenta – mobilní telefony, které již ve Finsku svou rozšířeností předstihly svého nepřenosného konkurenta. Kdo by si myslel ještě před pěti lety, že mladí lidé ve Spojených státech budou trávit více času u Internetu než u televize, která je právě pro Ameriku tak symbolická. Rychlost, to je jediné, v čem si můžeme být jisti. Rychlost změn se zvyšuje a jistě v nejbližší době zvyšovat bude. To se týká všech odvětví, bankovnictví nevyjímaje. A právě díky tomu, že změny jdou přes všechna odvětví, nejedná se o změny čistě technologické či technické. Banky budou měnit svou strategii společně s tím, jak se bude měnit okolní prostředí. I pro banky se trh začíná přerozdělovat. Pomalí začínají ustupovat rychlejším. Velcí se slučují a stávají se ještě většími, aby byli vybaveni ještě větší zbraní v podobě kapitálu než jejich konkurence. Očekávají obrovské investice do technologií a zároveň možnost snížení a rozředění nákladů na provoz.

Neuspějí pomalí a nepružní, protože prostředí je rychlé a pružné. Určitě neuspěje řada z těch, kteří jsou rychlí, ale nemají potřebnou míru znalostí nebo třeba jen štěstí. Dlouhodobě neuspějí ti, kteří si nedokáží dobýt významné postavení na trhu, nebudou partnery pro ostatní společnosti. Naopak uspějí ti, kteří dokáží skloubit rychlost s výrazným postavením na trhu a svou vlastní velikostí.

V současné době jsou dnes považovány za delikty nejvíce ohrožující informační systémy a data v nich uložená. Podle různých průzkumů incidentů týkajících se ITS (stavu informační bezpečnosti) ve světě a u nás lze zobecnit, že největšími hrozbami jsou:

1) únik citlivých informací v důsledku jednání zaměstnanců (aktivní krádež dat nebo nedbalostní prozrazení či umožnění úniku);
2) neoprávněný přístup do počítačové sítě organizace přes komunikační síť (typicky Internet) od narušitele zvenčí za účelem:
   a) získání informací
   b) neoprávněného užívání hardware a/nebo software
   c) poškození programů a/nebo dat v počítači uložených
   d) znemožnění užívání hardware, software a/nebo dat jiným osobám
3) virové napadení (zvenčí – obvykle přes Internet nebo zevnitř – nahrání infikovaného souboru zaměstnancem)

4) odposlech dat z interní sítě (LAN – local area network) nebo upraveného hardware (počítače, klávesnice, tiskárny apod.)
5) chyby zaměstnanců nebo dodavatelů (externistů) při instalacích hardware nebo software, při jejich užívání a/nebo údržbě
6) porušování autorských práv (úmyslně či z nedbalosti)
7) selhání důležitého sytému v důsledku poruchy hardware včetně komunikací nebo chyby v software nebo sabotáže (zevnitř, zvenčí)
8) výpadek v dodávce energie
9) krádež zařízení
10) živelní pohroma, požár, teroristický útok nebo jiný útok směřující především proti hmotnému majetku

Informatická kriminalita se více méně stává každodenní záležitostí podobně, jako se jí stala kriminalita hospodářská. Z hlediska kriminalistiky je velmi novým oborem, avšak akcelerace lidské společnosti v oblasti informačních technologií se promítá i do všech oborů: od obchodu služeb, přes umění či erotiku a pochopitelně i do nových forem trestné činnosti. Člověk je stále závislejší na bezchybném fungování informačních technologií a roste společenský požadavek na ochranu těchto technologií před zločinci. Tento požadavek je o to významnější, že počítačová kriminalita je stále více spojována s organizovaným zločinem. Důsledkem výše uvedených trendů je stále větší překrývání řady oborů. Zatímco zpočátku k tomu docházelo jen po linií oborů technických – např. počítače a komunikace, nyní je již propojování informačních, organizačních, společenských a dalších vazeb takové, že znalostní domény vyhrazené dříve pouze úzkým specialistům se začínají překrývat a propojovat. Odborníci působící v oblasti prevence a represe proti informatické a [83]počítačové kriminalitě budou muset disponovat právě takovými mezioborovými znalostmi od informatiky přes bezpečnost informačních systémů až po právní disciplíny. Moderní technologie dávají možnosti pachatelům trestné činnosti, komplikují život přece jen konzervativněji postupujícím orgánům činných v trestním řízení a teprve o hodně později se tyto technologie stávají vydatným pomocníkem v boji proti zločinu. Snahou všech zúčastněných odborníků by mělo být co největší zkrácení odstupu mezi „zloději“ a „četníky“ na poli informačních a telekomunikačních technologií.

[83] Scheinost, M. *Tři sondy k problematice organizovaného zločinu*. Praha IKSP,1995

9 SEZNAM POUŽITÝCH ZDROJŮ

1. AMBROŽ, J. *Jak silná je naše "softwarová policie"?* [online]. 24.5.2005 [cit. 2005-11-19]. Dostupný z WWW: <http://www.lupa.cz/clanky/jak-silna-je-nase-softwarova-policie>

2. Bibliografický záznam původní práce: PAUKERTOVÁ, Veronika. *Elektronická informační kriminalita [Electronic information crime]*. Praha, 2006. 114 s., 6 s. příl. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2006. Vedoucí diplomové práce PhDr. Richard Papík, PhD.

3. ČECHLOVSKÝ, V. – str. 14. *Co všechno už umějí bankomaty*.05.05.2007. Deník Právo

4. <http://www.cpufilm.cz>

5. Česko. Ministerstvo vnitra ČR. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení* [online][cit. 2005-23-07]. Dostupný z WWW: <http://www.mvcr.cz/dokumenty/technologie/uvod.html>

6. Česko. *Zákon o ochraně osobních údajů* [online] [cit. 2005-09-07]. Dostupný z WWW: <http://business.center.cz/business/pravo/ zakony/oou>

7. ČÍŽEK, V. – str. 17, - *Na platební kartě lze mít fotku dětí, přátel i svého psa*. Deník Právo.02.06.2007

8. *Čipy znemožní kopírování a zneužití karet*. Právo, 14. 12. 2002

9. *Čipové karty proti elektronickým zlodějům*. Právo, 10. 1. 2002. Podvody s platebními kartami stály klienty a banky miliony. Právo, 6. 11. 2002

10. DASTYCH, J. *Extremismus na Internetu* [online].11/2000 cit. 2006-03-16]. Dostupný z WWW: <http://www.interdata.cz/sluknovsko_cz/sluknovsko/noviny/rn/rn2000/clanek.php3?kod1=262&cislo=11&typ=>

11. DVOŘÁK, J.- KŘÍŽ, J.- DVOŘÁK, J. *Elektronický obchod.* Skripta VUT v Brně, Fakulta podnikatelská 2005

12. F.S.C. *Zavedení systému řízení informační bezpečnosti – ISMS.* [online]. [cit. 2006-02-12]. Dostupný z WWW: <http://www. fsc-ov.cz/produkt.php?id=106>.

13. FOLTZ, Bryan C. Cyberterrorism, computer crime and reality. *Information Management & Computer Security*. 2004, vol. 12, no. 2, s. 154-166

14. GRUBLOVÁ, E., - PRUSÁK, J, - PŘADKA, M, - STEINOVÁ, M. *Internetová ekonomika*. Ostrava.2002. ISBN 80 – 7329-000-6

15. HLAVENKA, J. *Phishing : když si hacker podá ruku se zločincem* [online]. 6.7.2004 [cit. 2004-12-16]. Dostupný z WWW <http://www.zive.cz/h/Uzivatel/AR.asp?ARI=117286>

16. HRADECKÝ, M. *Platební prostředky jejich ochrana a padělání.*Praha 2008. ISBN 80-7312-055-0

17. KŘÍŽ, L. *X-vize budoucí bezpečnosti* [online]. 1.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://www.computerworld.cz/cw.nsf/ID/B7AE352FC15C49A9C12570E9006B5837?OpenDocument&cast=1>

18. LÁTAL, I. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista*. 1998, č. 3, s. 3-15

19. MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. 97 s. ISBN 80-7226-419-2

20. LANDA, M. *Ekonomické řízení podniku.*Computer Prrss, a.s. Brno.2008. 198 s. ISBN 978-80-251-1996-9

21. McAfee. *Zpráva spoečnosti McAfee o virtuální kriminalitě : první celoevropská studie o organizovaném zločinu a internetu* [online]. 2004 [cit. 2006-01-13]. Dostupný z WWW: <http://www.fi.muni.cz/~xbitto/McAfee_kriminalita.pdf>

22. MOUČKA, B. - PEŠA, R. A zase spam [online]. *Zpravodaj ÚVT MU*. 2004, roč. 14, č. 5, s. 17-19. Dostupný z WWW: <http://www.ics.muni.cz/bulletin/issues/vol14num05/pesa/ pesa.html>

23. NAJMAN, M. *Jak stahovat* [online]. 30.1.2006 [cit. 2006-02-10]. Dostupný z WWW: <http://aktualne.centrum.cz/clanek.phtml?id=64780>.

24. PORADA, V. Kriminalita v digitálním prostředí a trendy aktuálních hrozeb. *Karlovarská právní revue.* 2005, č. 3, s.12-29

25. POŽÁR, J. Některé trendy informační války, počítačové kriminality a kyberterorismu. In *Bezpečnost v podmínkách organizací a institucí ČR : sborník z mezinárodní konference, 20. května 2005, Praha* [online]. Praha : Soukromá VŠ ekonomických studií, 2005. ISBN 80-86744-49-3. Dostupný z WWW: <http://www.svses.cz/stahni/sbornik.pdf>

26. *Připravované novinky v oblasti platebních karet KB* – tisková zpráva 2007

27. PROSISE, Ch. - MANDIA, K. *Počítačový útok : detekce, obrana a okamžitá náprava.* Praha : Computer Press, 2002. 432 s. ISBN 80-7226-682-9

28. PŘIBYL, T. Hacker: *Klávesnice jako zbraň*: rozhovor s nejslavnějším hackerem světa Kevinem Mitnickem. *PC World.* 2003, č. 11, s. 38-43

29. PŘIBYL, T. Informační bezpečnost v roce 2004. *PC World Security.* 2005, č. 1, s. 2-7

30. PŘIBYL, T. Po phishingu přichází pharming. *Computerworld.* 2005, č. 27, s. 28-29

31. Institut ministerstva spravedlnosti pro další vzdělávání soudců a státních zástupců: *Trestná činnost v bankovním sektoru*, 2. vyd. – Praha 1997. 187 s. ISBN 80-7256-482-3

32. Institut ministerstva spravedlnosti pro další vzdělávání soudců a státních zástupců: *Trestná činnost na českém kapitálovém trhu*, 1 – vyd. Praha 1997. 115 s. ISBN 80-71214-493-5

33. JUŘÍK, P. *Svět platebních karet* - bankovnictví: 1. díl 1995. 618s. ISBN 80-248-0194-1

34. JUŘÍK, P. *Svět platebních a identifikačních karet*. 1999. 465s. ISBN 80-247-0081-6

35. JUŘÍK, P. *Platební karty*: 1870 – 2006: velká encyklopedie 2006. 312s. ISBN 80-214-3255-1

36. JUŘÍK, P. *Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet.* 1. vyd. Praha 2003. 312s. ISBN 80-7201-311-4

37. KONEČNÝ, M. *Metodologie vědy a výzkumu.* 1. vyd.. Brno: Fakulta podnikatelská, VUT v Brně, 1993. 91 S. Bez ISBN

38. KOSIUR, D. *Elektronická komerce*. Principy a praxe. 1 . vyd. Brno: Computer Press, 1998. 267 s. ISBN 80-7226-097-9

39. KUCHAŘ, M. *Bezpečná síť*. Jak zajistíte bezpečnost vaší sítě. 1. vyd. Praha: Grada Publishing, 1999. 92 s. ISBN 80-7169-886-5

40. *Kreditní kartu je lepší někdy nechat doma* 4. 8.2007 - (vč.) - str. 18

41. RAK, R; - PORADA, R. Pohled na bezpečnostní hrozby v informatice a telekomunikacích na přelomu roku 2004/2005. *Bezpečnost v podmínkách organizací a institucí ČR : sborník z mezinárodní konference, 20. května 2005, Praha* [online]. Praha: Soukromá VŠ ekonomických studií, 2005. ISBN 80-86744-49-3. Dostupný z WWW: <http://www.svses.cz/stahni/sbornik.pdf>

42. SADOVSKÝ, D.: *Odhalování trestné činnosti na úseku platebních karet*. Diplomová práce, PA ČR, Praha, 2003

43. SCHLOSSBERGER,O. *Platební styk.* Praha 2005. ISBN 80-7265-072-6

44. SOFRON, S.: *Čipové platební karty*. Odborná sdělení kriminalistického ústavu, 1999, 3, s. 10 – 13

45. SMEJKAL, V. *Informační a počítačová kriminalita v České republice* [online]. [cit. 2004-12-16]. Dostupný z WWW: <http://www.mvcr.cz/casopisy/studie/diskuse/analyza.html>

46. SMEJKAL, V. *Právo informačních a telekomunikačních systémů*. Praha: C. H. Beck, 2004. xxx, 770 s. ISBN 80-7179-765-0

47. SCHEINOST, M. *Tři sondy k problematice organizovaného zločinu*. Praha: IKSP, 1995. KADEŘÁBKOVÁ, D. *Hospodářská kriminalita ve finanční oblasti*. Praha: IKSP, 1995. CEJP, M. *Druhy a formy činnosti organizovaného zločinu*. Praha.1995: IKSP, 1996. BUDLA, I. *Organizovaná kriminalita v ČR a v USA – kriminologické a právní aspekty*. Praha: IKSP, 1996

48. SVATOŠOVÁ, H. *P2P sítě : přísné pojetí odpovědnosti podle Nejvyššího soudu USA zákon* [online]. 5.7.2005 [cit. 2005-10-13]. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=288275>

49. SVETLÍK, M. Informační bezpečnost: část 1-4. *Softwarové noviny*. 2002, č. 2-5

50. ŠÁMAL, P. *Podnikání a ekonomická kriminalita v České republice*. 1.vyd. - Praha: C.H.Beck, 2001 - xxv, 776 s. ISBN 80-7179-493-7

51. TICHÝ, J. – *Loni proběhlo 140 miliónů operací přes platební karty*. Deník právo.12.05.2007

52. TOLAR, O. *Policie je krátká na weby popírající holocaust* [online]. 22.2.2006 [cit. 2006-02-26]. Dostupný z WWW: <http://zpravy.idnes.cz/krimi.asp?r=krimi&c=A060222_114752_krimi_ton>

53. Úmluva o potírání penězokazectví, Ženeva 20.4.1929, vyhlášena ve Sbírce zákonů číslo 15/1932 Sb.

54. Věstník České národní banky10 z 19.5.1994 jímž se vydává Úřední sdělení ČNB – výklad k vybraným ustanovením zákona o platebním styku

55. VONDRUŠKA, P. Hackeři, crackeři, rhybáři a lamy. *Cryptoworlds* [online]. 2004, č. 7-8, s. 4-12. [cit. 2004-12-16]. Dostupný z WWW: <http://www.crypto-world.info/casop6/crypto78_04.pdf>

56. Vyhláška České národní banky č. 523/2006 Sb., o podmínkách, za kterých lze reprodukovat bankovky, mince, šeky, cenné papíry a platební karty a vyrábět předměty, které je úpravou napodobují.

57. Výkladové stanovisko NSZ č. 2/2007

58. YANG, Susan; AITEN, Dave. *The hacker's handbook : the strategy behind breaking into a defending networks*. Boca Raton: Anerbach, c 2004. xxxiv, 860 s. ISBN 0-8493-0888-7

59. Zákon č. 140/1961Sb., trestní zákon ve znění následně vydaných novel

60. Zákon č. 200/1990 Sb., o přestupcích, část druhá – Zvláštní část

61. Zákon České národní rady č. 6/1993 Sb., o České národní bance ve znění následně vydaných novel

62. Zákon č. 21/1992 Sb., o bankách

63. Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku) ve znění zákona č. 257/2004Sb.

64. Zákon č. 191/1950 Sb., Zákon směnečný a šekový

65. ZZ PP ČR č. 130/2007, kterým se upravuje postup Policie ČR při plnění úkolů v trestním řízení ve znění následně vydaných novel.

66. ZPPP ČR č. 81/2003, kterým se upravuje postup policie ČR při prověřování a vyšetřování trestných činů v případech výskytu penězokazectví ve znění následně vydaných novel.

67. Výkladové stanovisko NSZ č. 2/2007

68. Webová stránka České národní banky www.cnb.cz (česká platidla)

69. Webová stránka Evropské centrální banky www.ecb.int (ochranné prvky eurobankovek)

70. Webová stránka http://peníze.navajo.cz

71. Webová stránka www.penize.cz/nástroje/bankovky

72. Webová stránka www.mesec.cz/texty

73. Webová stránka www.penize.cz/produkty/platebni-karty

74. Webová stránka www.penize.cz/produkty/platebni-karty/texty/1969/platebni-karty-a-jejich-druhy/?IDP=1

75. Webové stránky www.bankovnikarty.cz

76. Webová stránka www.jcbinternational.com

77. Webová stránka Bezpečnostního výboru bankovních karet v ČR www.bankovnikarty.cz/vyrocni_zprava/vyrocni_zpravasbk_2006.pdf

78. Webové stránky www.ceed.cz/bankovnictvi/767seky.htm

79. Webové stránky www.mesec.cz/texty/seky

80. Webová stránka Státní tiskárny cenin www.stc.cz

81. Webová stránka www.cnb.cz/cz/platidla/padelky

82. Webová stránka www.bankovnikarty.cz/data/cm3_2005.pdf (elektronické verze magazínu Cardmag vydávaných Sdružením bankovních karet)

83. Webová stránka www.BSA.cz. říjen 2006

SEZNAM POUŽITÝCH ZKRATEK

B2C	- obchod mezi podnikateli (Business to Business)
B2B	- prodej podnikatele spotřebiteli (Business to Consumer)
C2C	- prodej mezi nepodnikateli, res. Občany (Consumer to Consumer)
CRM	- řízení vztahů se zákazníky (Customer Relationship Management)
EIK	- elektronická informační kriminalita
ICT	- informační a komunikační technologie
IB	- informační bezpečnost
IS	- informační systém
IT	- informační technologie
ITS	- informační a telekomunikační systém
ObčZ	- zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů
ObchZ	- zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů
PIN	- autentizační kód ve formě čísla (personal Identification Number)
POIZ	- zákon č. 283/1991 Sb., o Policii české republiky, veznění pozdějších předpisů
PřesZ	- zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů
P2P sítě	- klient-klient, označení architektury počítačových sítí
SCM	- řízení všech procesů v rámci dodavatelského řetězce počínaje zajištěním surovin pro první článek řetězce přes zhotovení produktu a konče dodávkou konečnému spotřebiteli posledním článkem řetězce (Supply Chain management)
TrZ	- trestního zákona
ÚSKPV	- útvary služby kriminální policie a vyšetřování
WWW stránka	- je dokument, který se nachází na určitém webovém serveru, jeho obsah je propojen pomocí hypertextových odkazů na jiná místa v tomto dokumentu, v jiných dokumentech na tomto serveru nebo zcela na jiných serverech nacházejících se v pavučině internetu kdekoliv na světě

SEZNAM PUBLIKACÍ

Příspěvky na konferencích

1. ŠULC, V. *Platební karty a jeho možnosti zneužití,* KOLOKVIA Fakulta podnikatelská VUT v BRNĚ. 2006. ISBN: 80-214-3063-X

2. ŠULC, V. *Zneužití platebních karet*, MendelNet v Brně, 2007. ISBN 978-80-903966-6-1

3. ŠULC, V. *Konkurenceschopnost podniků.* Masarykova univerzita, ekonomicko – správní fakulta v Brně, 2007. ISBN 80-276-1056-1

4. ŠULC, V. *Platební karty-novinky v bezhotovostním styku*. In Festive Scientific Conference on the Occasion of 15 th Anniversary of the Establishment of Faculty of Business and Management Brno University of Technology. Brno: VUT v Brně, FP, 2007. ISBN 978-80-214-3482-0

5. ŠULC, V. *Strategie firmy pro elektronický obchod – počítačový virus platebních karet.* MendelNet PEF. Brno, 2008. ISBN 978-80-87222-03-4

6. ŠULC, V. *Konkurenceschopnost podniků*., Masarykova univerzita , ekonomicko – správní fakulta v Brně,1. vydání, 2008. ISBN 978-80-210-4521-7

7. ŠULC, V. Strategie firmy pro elektronický obchod – novinky bezkontaktní platby prostřednictvím technologie Master Card PayPass. Univerzita Tomáše Bati ve Zlíně. 2008. ISBN 978-80-7318-663-0

8. ŠULC, V. Strategie firmy pro elektronický obchod – Skimming platebních karet. Fakulta podnikového manažmentu EU v Bratislave, 2008. „ Ekonomika, financie a manažment podniku II.“ ISBN 978 -80-225-2628-9

PŘÍLOHY

Příloha č.1 – Slovníček pojmů v oblasti platebních karet – výběr

Příloha č.2 – Bankomaty, platební karty

Příloha č.3 – Stanovisko NSZ

Příloha č.4 – Poznámky

Příloha č.5 – Curriculum vitae

Příloha č.6 – Další literatura

Příloha č. 1 - Slovníček pojmů v oblasti platebních karet – výběr

(viz. www.bankovnikarty.cz/web_sbk/czech/menu/slovnik_cz.htm)

Pojem česky	Pojem anglicky	Vysvětlení
3D secure	3D secure	Protokol definující pravidla pro bezpečné platby na internetu z pohledu všech tří účastníků transakce - držitele, obchodníka a platebního systému. Je podporovaný všemi kartovými asociacemi.
Acquirer	Acquirer	Zúčtovací banka, která uzavírá smluvní vztahy s obchodními společnostmi, zpracovává transakce platebními kartami (přímo nebo prostřednictvím třetí strany) a zajišťuje clearing a zúčtování.
Akceptace karet	Acquiring	Proces realizace transakcí provedených platební kartou (bezhotovnostní platba u obchodníka, výběr hotovosti z bankomatu nebo v bance). Je podmíněna udělením příslušné licence od mezinárodní kartové asociace (MasterCard International, VISA International, Diners Club, American Express, JCB).
Aplikace	Application	Sada softwarových instrukcí a dat ve formě počítačového programu určeného k provedení konkrétních funkcí. U čipových karet to je konkrétní sada instrukcí a souvisejících dat používaná čipem pro interakci s terminálem k provedení transakce.
ATM	ATM	Zkratka pro Automated Teller Machine, viz Bankomat.
ATM Off-site	ATM Off-site	Označení pro bankomat, umístěný mimo budovu banky.
Autentikační požadavek	Authentication request	Požadavek na autentikaci držitele karty zaslaný obchodníkem v protokolu 3-D Secure vydavateli, který je také pro tento protokol certifikován.
Autentikační procedura	Autenthication procedure	Proces ověřující oprávněnost držitele karty k jejímu použití nebo oprávněnost obchodníka k akceptaci karet.
Autentikační prvek	Autenthication element	Prvek, podle kterého se ověří oprávněnost držitele karty k jejímu použití nebo oprávněnost obchodníka k poskytování služeb.
Autorizace	Authorisation	Proces, při kterém je vyžádán souhlas vydavatele karty s platbou nebo výplatou hotovosti prostřednictvím platební karty. Souhlas je vyjádřen poskytnutím autorizačního kódu.Pozn. Obecně o schválení nebo zamítnutí transakce rozhoduje vydavatel nebo třetí strana, jednající jménem vydavatele. U čipových transakcí může schválení vydat čip v rámci limitů stanovených vydavatelem.
Autorizační centrum	Authorisation centre	Poskytuje autorizační služby jednomu nebo více členům kartové asociace.
Autorizační kód	Authorisation code	Autorizační kód je alfanumerický kód, vyjadřující souhlas vydavatele karty s provedením transakce. Pozn. Kód generuje vydavatel, pokud byla schválena žádost o autorizaci. Autorizační kód slouží jako důkaz o poskytnutí souhlasu vydavatele s uskutečněním transakce. U čipových karet kód nebo kryptogram může generovat čip a je uvedený v autorizační odpovědi, pokud je čipem transakce schválena.
Autorizační	Authorisation	Zpráva poslaná vydavatelem zúčtovací bance, která obsahuje odpovědní

odpověď	response	kód informující zpracovatelskou banku, jak při transakci dále postupovat.
Autorizační služba off-line	Off-line authorisation service	Proces vyhodnocení a schválení provedení transakce na terminálu v prodejním místě, a to bez kontaktování vydavatele.
AVS	AVS	Address Verification System - zkratka pro automatický systém umožňující obchodníkům, kteří akceptují transakce bez přítomnosti karty (CNP) vzdálenými kanály, např. telefonem, písemnou objednávkou nebo internetem, ověřit zúčtovací adresu držitele karty (Systém je využíván převážně v USA).
BankNet	BankNet	Komunikační síť kartové asociace MasterCard, která se používá ke směrování (routing) všech interregionálních transakcí MasterCard založených na podpisu.
Bankomat	Cash dispenser	Samoobslužné zařízení umožňující výběr hotovosti prostřednictvím platební karty, případně přístup k dalším bankovním službám. Ve zkratce též ATM.
Bezpečnostní prvky	Security features	Bezpečnostní prvky chránící platební kartu před padělaním; např. hologram, speciální ultrafialový tisk, atd.
BIN	BIN	Bank Identification Number – bankovní identifikační číslo, což je jedinečná série čísel přidělená platebním kartovým systémem hlavním členům asociace. BIN identifikuje typ kartového produktu a současně instituci, která kartu vydala.
Biometrika	Biometrics	Biometrika označuje biometrické metody identifikace, které využívají měření unikátních lidských charakteristik k ověření identity jedince, např. otisku prstu, skenování oka či dynamiky podpisu.
CAM	CAM	Metoda autentikace karty / Card Authentication Method. Proces, kterým je platební karta ověřena jako právoplatná, nikoli padělaná. Pozn. U karty s magnetickým proužkem zahrnuje např. kontrolu hologramu, který může být zkontrolován obchodníkem, resp. zašifrovaných dat na magnetickém proužku, která může zkontrolovat vydavatel karty. V anglické zkratce CAM.
CEMEA	CEMEA	Region Central and Eastern Europe, Middle East, and Africa.
Centralizované přijímání karet	Central acquisition	Služba, umožňující držiteli licence od kartové asociace, aby zajišťoval přijímání karet od mezinárodní obchodní společnosti působích v různých zemí (například mezinárodní letecké společnosti nebo půjčovny automobilů).
Certifikace	Certification	Proces používaný v kryptografii veřejného klíče, při kterém majitel veřejného klíče předkládá tento klíč pověřené instituci, aby jej tato instituce digitálně podepsala. Výsledek majitel obdrží ve formě certifikátu veřejného klíče. Proces používaný kartovou asociací k testování a certifikaci systémů členů asociace před uvedením do živého provozu.
Certifikační autorita	Certification authority	Centrální autorita v kryptografickém systému veřejného klíče, která je pověřena, aby digitálně podepisovala veřejné klíče náležející jednotlivým účastníkům onoho systému, a která posílá výsledky ve formě certifikátů

		veřejného klíče.
Certifikát veřejného klíče	Public key certificate	Bezpečnostní token používaný v kryptografii veřejného klíče, který má formu veřejného klíče digitálně podepsaného pověřenou autoritou. Příjemce takového certifikátu je schopen odvodit hodnotu veřejného klíče, jakou představuje, a verifikovat autenticitu a oprávněného vlastníka tohoto veřejného klíče.
Cirrus	Cirrus	Mezinárodní program sdílení bankomatů vlastněných MasterCard International a provozovaných společností Cirrus System Incorporated (dceřiná společnost ve stoprocentním vlastnictví). Programu Cirrus se mohou zúčastnit jak karty MasterCard, tak i výlučné debetní a kreditní karty bank, což držitelům karet umožňuje přístup do sítě mezinárodně sdílených bankomatů, známé jako Síť bankomatů Cirrus (Cirrus ATM Network).
Clearing	Clearing	Proces výměny údajů o finanční transakci mezi acquirerem a vydavatelem k umožnění zaúčtování transakce na účet držitele karty a rekonciliace pozice člena asociace k vypořádání.
Clearingová data	Clearing data	Údaje, týkající se realizované transakce; případně se použijí jako podklad k reklamaci prostředků od člena asociace, který byl při transakci protistranou.
Clearingové centrum	Clearing centre	Instituce, kterou používají vydavatelé a zúčtovací banky v dané zemi jako své centrum pro zpracování a nepeněžní vypořádání finančních transakcí.
CLIP	CLIP	Viz Elektronická peněženka.
Co-brandovaná karta	Co-branded card	Platební karta, vydaná v rámci partnerského programu s jiným subjektem.
Compliance	Compliance	Proces, při kterém kartová asociace rozhodne spor mezi členy asociace, plynoucí z porušení pravidel asociace. Jde o konečnou instanci reklamačního řízení, kdy navrhující člen může osvědčit, že došlo nebo může dojít k finanční újmě na konkrétním účtu čísla karty a v rámci reklamačního řízení nebyl dostupný žádný kód důvodu pro chargeback a pokus vyřešit záležitost "v dobré víře" nebyl úspěšný.
CSC	CSC	Card Security Code / Bezpečnostní kód karty. Viz Kontrolní kód.
CV	CV	Card Validation. Viz Kontrolní kód.
CV1	CV1	Část kontrolního kódu uložená na magnetickém proužku karty. Viz Kontrolní kód
CV2	CV2	Část kontrolního kódu vytištěná na podpisovém proužku karty. Viz Kontrolní kód.
CVC	CVC	Card Validation Code / Kód ověření karty. Název pro kontrolní kód používaný asociací MasterCard. Viz Kontrolní kód.
CVM	CVM	Viz Metoda ověření držitele karty / Cardholder Verification Method.
CVV	CVV	Card Validation Value / Hodnota ověření karty. Název pro kontrolní kód používaný asociací VISA. Viz Kontrolní kód
Čipová karta	Chip card, smart card, ICC, karta IC	Platební karta, která je vybavena čipem s programovatelným mikroprocesorem a pamětí. Čipová technologie nabízí zvýšení bezpečnosti a rozšíření funkcí karty (např. věrnostní programy, elektronická

		peněženka). Viz ICC.
Čipová transakce	Chip transaction	Typ transakce, která vzniká použitím čipové karty v čipovém terminálu a čipová data jsou načtena přímo z karty.
Čipový terminál	Chip terminal	Typ terminálu, certifikovaný podle specifikace EMV, který je schopen realizovat čipové transakce i transakce z magnetického proužku.
Číslo karty	Card number	Číslo, které je vyraženo (embosováno) a/nebo zašifrováno na platební kartě a které identifikuje vydavatele a konkrétní účet držitele karty. Pozn. Číslo karty se skládá z hlavního identifikátoru odvětví, identifikátoru vydavatele, identifikátoru konkrétního účtu a kontrolní číslice. Též označováno jako PAN, viz PAN.
Čítač pokusů o PIN	PIN try counter	Bezpečnostní mechanismus, používaný k omezení počtu pokusů o zadání PIN, které smí držitel karty provést (obvykle omezeno na tři pokusy). Pozn. Čítač slouží k zaznamenání počtu nesprávných zadání PIN pro transakci; hodnota čítače pokusů o PIN je počet zbývajících povolených pokusů o PIN. Tento čítač slouží k tomu, aby PIN nemohl "uhádnout" podvodník, který by opakovaně zadal mnoho různých kombinací PIN.
Členská a licenční smlouva	Membership and licence agreement	Smlouva mezi kartovou asociací a členem, která poskytuje statut člena a umožňuje členovi získat licenci na jednu nebo několik značek asociace.
Data stopy	Track data	Informace zašifrované do stopy 1, 2 nebo 3 magnetického proužku karty. Tato data sbírá (tj. čte) terminál při zahájení transakce spojené se čtením karty a jsou použita při následujících zprávách o autorizaci a clearingu transakce.
Database hacking	Database hacking	Neoprávněné vniknutí do databáze spravované třetí stranou.
Datový prvek	Data element	Specifické množství dat obvykle obsažených ve zprávách o autorizaci a clearingu, které má definovanou délku, formát, strukturu a povolený obsah a je identifikováno konkrétním číslem. Hlavní datové prvky používané k sestavení zpráv vyměňovaných mezi zúčtovací bankou a vydavatelem ISO 8587 (1987 a 1993) a dokumentace asociace na ně odkazuje číslem datového prvku. Používání strukturovaných datových prvků umožňuje automatické zpracování zpráv jak komunikační sítí, tak příjemcem dat.
Datum konverze	Conversion date	Datum účinnosti, kdy je částka (například částka transakce) konvertována z jedné měny do druhé s použitím relevantního měnového kurzu platného v onen den.
Datum předložení	Deposit date	Datum, kdy zúčtovací banka obdrží od obchodníka transakční doklad.
Datum převodu rubopisem	Endorsement date	Jedná se datum, kdy byla transakce (tj. údaje o transakci) poprvé vložena do výměnného systému (Interchange) a odeslána.
Datum transakce	Transaction date	Datum, kdy se realizuje transakce (tj. skutečné datum, kdy držitel karty kupuje zboží nebo služby nebo získává hotovost).
Datum valuty	Value date	Datum, kdy se finanční prostředky převedené na účet držitele karty stanou pro něj reálně dostupnými.
Datum vypořádání	Settlement date	Datum, kdy jsou převedeny finanční prostředky k vypořádání mezi zúčtovací bankou a vydavatelem.

Debetní karta	Debit card	Debetní karta je platební karta umožňující čerpat vlastní prostředky uložené na běžném nebo obdobném účtu
Doklad o transakci	Transaction Record	Papírový doklad, vydaný terminálem v místě transakce.
Držitel karty	Cardholder	Fyzická osoba, které byla na žádost a se souhlasem majitele účtu vydána platební karta k používání. Podepsáním smlouvy se držitel karty zavazuje dodržovat obchodní podmínky vydavatele karty. Držitel karty je identifikován číslem karty (kartového účtu).
Důvěrný údaj	Confidential Data	Údaj uvedený ve smlouvě o vydání platební karty sloužící k ověření držitele karty při její aktivaci, případně pro další komunikaci s bankou.
EFT POS	EFT POS	Electronic Funds Transfer at Point of Sale / Elektronický přenos dat v místě prodeje. Výraz pro elektronický platební terminál umožňující přečíst data z karty a odeslat data o transakci zpracovateli.
Elektronická peněženka	Electronic purse	Elektronická peněženka je elektronický platební prostředek (ve smyslu zákona 124/2002 Sb.), který obsahuje elektronickou hodnotu směnovanou za zboží a služby. Umožňuje mít na kartě uloženou peněžní hodnotu, která se při každém nákupu sníží, aniž by bylo třeba další autorizace. Po vyčerpání elektronické hodnoty se může opětovně předplatit nebo znehodit.
Elektronické obchodování	Electronic commerce	Druh obchodní transakce, při níž jsou transakce prováděny prostřednictvím internetu, kdy nakupující a obchodník nejsou na stejném fyzickém místě, a která zahrnuje platbu prostředky elektronického obchodování. Provádí se prostřednictví internetu přijímáním on-line transakcí (v prostředí bez přítomnosti karty), často iniciovaných držitelem karty ze zákazníkova osobního počítače. Také označováno jako e-obchodování, e-commerce.
Elektronický imprint	Electronic Imprint	Přečtení a vytištění nebo zachycení údajů o kartě terminálem čtoucím magnetický proužek nebo zařízením čtoucí čip.
Elektronický platební prostředek	Electronic Payment Means	Elektronickým platebním prostředkem je (ve smyslu zákona 124/2002 Sb.) a) prostředek vzdáleného přístupu k peněžní hodnotě, při jehož užívání se zpravidla vyžaduje identifikace držitele osobním identifikačním číslem přiděleným vydavatelem nebo identifikace jiným způsobem (představovaný platební kartou, mobilem s bankovním čipem atd.) b) elektronický peněžní prostředek (např. elektronická peněženka).
Elektronický transakční doklad	Electronic Transaction Receipt	Transakční doklad vytvořený elektronicky v prostředí s přítomností karty, kdy terminál generuje požadované údaje tištěné na transakčním dokladu.
Embosování	Emboss	Proces vyznačení identifikační údajů na kartě ve formě prolisovaných nebo vyrytých znaků.
EMV	EMV	Technické specifikace vyvinuté pod gescí společnosti EMVCo (Europay International, Mastercard International a VISA International) k zavedení

		standardů pro zpracování debetních a kreditních transakcí a k zajištění globální interoperability používání čipové technologie v platebním styku.
EMVCo	EMVCo	Odvětvová zkratka pro konsorcium tří společností (Europay, MasterCard a Visa), které mají ve společné gesci globální standardy pro elektronické finanční transakce. Také se používá pro technické specifikace vydané tímto konsorciem, schválené všemi třemi společnostmi a určené k zajištění globální interoperability čipových karet, čipových terminálů, finančních zpráv a souvisejících služeb.
Eurocheque	Eurocheque	Standardizovaná forma bankovního šeku, který se může používat v různých evropských zemích jako prostředek platby za zboží a služby nebo může být inkasován v bance.
Europay	Europay	Evropská kartová asociace, společnost Europay International S.A., v roce 2002 splynula se společností MasterCard International.
Exception File	Exception File	VISA: Soubor ve formátu VISANet obsahující čísla karet, ke kterým vydavatel předurčil autorizační odpověď, a ke kterým má autorizující účastník sítě on-line přístup.
Fiktivní číslo karty	Fictious Account number	Číslo platební karty (resp. číslo kartového účtu), které nikdy neexistovalo.
Firemní karta	Business card	Platební karta vydaná malému podniku pro jeho zaměstnance k placení podnikových výdajů (obvykle až pro 10 zaměstnanců společnosti s uvedením jména oprávněné osoby na kartě). Podle dohody se účtování provádí na vrub účtu společnosti nebo soukromého účtu zaměstnance. Viz též Corporate card.
Globální kobrandované partnerství	Global Co-branding Partnership	Smluvní vztah mezi vydavatelem a globálním kobrandovaným partnerem.
Hlasová autorizace	Voice authorisation	Služba, kterou poskytují acquireři obchodníkům, umožňující zatelefonovat do centra hlasové autorizace a získat autorizaci pro manuální transakce přesahující limit prodejny. Používá se také jako alternativní prostředek autorizace, jestliže se terminál nemůže připojit k acquirerovi on-line. V takovém případě obchodník zatelefonuje do centra hlasové autorizace a telefonicky uvede relevantní informace o kartě a transakci. Poté centrum hlasové autorizace pošle žádost o autorizaci on-line vydavateli a sdělí obchodníkovi autorizační kód od vydavatele karty. Tento kód zaznamená obchodník na prodejní doklad.
Hlavní licence	Principal licence	Právo poskytnuté členovi asociace, který se nazývá "majitel hlavní licence" (principal licensee), na používání ochranné známky nebo známek, jak stanovuje příslušná licenční smlouva a v souladu s produktovými pravidly platnými pro ochrannou známku(-y).
Hologram	Hologram	Laserem pořízený snímek, který vytváří trojrozměrný obraz. Používá se u platebních karet jako preventivní opatření proti padělání.
Hostitelský systém acquirera	Acquirer host system	Počítačový a komunikační systém, který umožňuje zpracovávat transakce s větším počtem instrukcí nebo může zpracovávat transakce jen pro jednoho zpracovatele. Pozn. Hostitelský systém (AHS=Acquirer Host System) může přímo nebo nepřímo podporovat terminály v obchodních společnostech a vyměňuje si zprávy s komunikační sítí asociace a s vydavateli prostřednictvím modulu

		acquirera. V mnoha případech se výrazy "acquirer" a "acquirerův hostitelský systém" používají ve stejném významu.
Hostitelský systém vydavatele	Issuer host system	Počítačový a komunikační systém, který členovi asociace poskytuje zpracovatelské funkce vydavatele. Pozn. Hostitelský systém vydavatele (IHS=Issuer host system) může zpracovávat transakce pro větší počet institucí nebo může zpracovávat transakce pro jednotlivého člena. Hostitelský systém vydavatele používá zprávy standardní aplikace ISO 8583 ke komunikaci se sítí asociace a s acquirery prostřednictvím modulu vydavatele. V mnoha případech se místo "hostitelský systém vydavatele" může používat termín "vydavatel" a naopak.
Hybridní karta	Hybrid card	Hybridní karta je platební karta vybavená jak magnetickým proužkem, tak čipem pro záznam dat a komunikaci s terminály. Pozn. Hybridní karty fungují jako čipové karty na terminálech podporující čip a jako karty s magnetickým proužkem na ostatních terminálech.
Hybridní terminál	Hybrid terminal	Zařízení pro akceptaci karet, které podporuje magnetický proužek i čipovou technologii, splňuje výkonnostní standardy asociací) a je schopné podporovat klávesnici PIN.
Charge karta	Charge card	Charge karta je platební karta s odloženou splatností. Jedná se o úvěrovou kartu s možností placení do výše povoleného úvěrového rámce a čerpané prostředky nejsou až do splatnosti čerpané částky úročeny.
ICA	ICA	MasterCard: Zkratka Interbank Card Association (Mezibankovní karetní asociace). Jedinečné čtyřčíselné identifikační číslo přidělené platebním kartovým systémem finanční instituci, zpracovateli, třetí straně nebo jinému typu klienta pro jednoznačnou identifikaci tohoto klienta.
ICC	ICC	Integrated Circuit Card (karta s integrovaným obvodem). Platební karta, která obsahuje uložený integrovaný obvod neboli čip. Používá se také anglické označení "smart card" nebo "chip card" (čipová karta). Viz Čipová karty / chip card.
Inteligentní detekční systém	Inteligent detection system	IT systém používaný bankami, který napomáhá rozpoznat podvodné používání platební karty dříve, než je její ztráta zjištěna držitelem a ohlášena. Jedná se o systém založený na bázi existujících znalostí nebo využívající samoučící se mechanismy.
Interchange	Interchange	Výměna dat o transakcích a záznamech o zúčtování mezi zúčtovacími bankami a vydavateli podle definovaných pravidel. Z hlediska území se jedná buď o domácí interchange nebo mezinárodní interchange.
Karta MasterCard	MasterCard card	Kartový produkt asociace MasterCard, který nabízí MasterCard International svým členům. Logo MasterCard na přední nebo zadní straně karty zaručuje globální akceptaci. Na kartě může být také podle volby vydavatele vytištěn jeho název. Tyto karty umožňují svým držitelům nakupovat zboží a služby a vybírat hotovost v bankomatech.
Karta VISA	Karta VISA	Kartový produkt asociace VISA, který nabízí VISA International svým členům. Logo VISA na přední nebo zadní straně karty zaručuje globální akceptaci. Na kartě může být také podle volby vydavatele vytištěn jeho název. Tyto karty umožňují svým držitelům nakupovat zboží a služby a vybírat hotovost v bankomatech.
Kartová asociace	Card association	Organizace, která řídí a standardizuje provoz a zúčtování transakcí platebními kartami pod svou značkou, např. MasterCard, VISA, Diners

		Club International, American Express, JCB.
Kartový podvod	Card fraud	Podvod spáchaný s využitím platební karty nebo znalostí obsahu jejích dat.
Kategorie obchodníka	Merchant category	Klasifikace typu obchodu nabízeného nebo prováděného obchodníkem.
Klávesnice PIN	PIN pad	Malá klávesnice, která je součástí elektronického platebního terminálu a na které může držitel karty zadat svůj PIN za účelem verifikace držitele karty.
Kobrandovaná karta	Co-branded card	Karta vydaná členem společně s obchodní společností a nesoucí loga obou organizací. Společná karta více značek je zaměřena na zákaznickou základnu konkrétního obchodníka, poskytovatele služeb nebo jiné komerční organizace.
Kód důvodu	Reason code	Numerický kód používaný v platebních zprávách a v záznamech transakčních dat k udání důvodu, proč byla provedena nebo požadována určitá akce.
Kód kategorie obchodníka	Merchant category code	Čtyřmístný číselný kód používaný k identifikaci typu obchodníka zapojeného do transakce. Kódy jsou stanoveny ISO a používají se v celém odvětví platebního styku, ve všech typech zpráv a výkazů. Ve zkratce MCC.
Kód měny	Currency code	Trojčíselný kód použitý k označení konkrétní měny ve finanční transakci (například měny transakce, měny použité k vystavení faktury držiteli karty, měny vypořádání apod.). Kartové asociace používají numerické ISO kódy měny.
Kód odezvy	Response code	Kód udávající statut transakce nebo zpráv nebo označující provedenou nebo požadovanou akci. Například v odpovědních zprávách o autorizaci odpovědní kód sděluje, zda byla transakce schválena nebo odmítnuta.
Kód země	Country code	Kód používaný k identifikaci konkrétního státu podle ISO seznamu mezinárodně používaných numerických a alfabetických kódů států. Používá se v elektronických zprávách k identifikaci konkrétního státu.
Kód zpracování	Processing code	Kód užívaný ve zprávách o platbách a záznamech o transakcí k identifikaci různých typů transakcí (nákup zboží, výběr z bankomatu apod.) a účtových převodů (z účtu nebo na účet držitele karty).
Kontrolní číslice	Check digit	Prostředek, jímž lze verifikovat integritu čísla karty nebo obsahu magnetického proužku. Jedná se o číslici vypočtenou Lühnovým algoritmem, která je součástí např. čísla karty.
Kontrolní kód	CV, CVC, CVS, CVV	Bezpečností prvek určený k tomu, aby zabránil falšování nebo manipulaci s údaji na kartě. Je uložen na magnetickém proužku (CV1) a vytištěn na podpisovém proužku karty (CV2).
Kreditní karta	Credit card	Platební karta sloužící k čerpání sjednaného úvěrového rámce, s individuálně stanovenými podmínkami splácení.
Libanonská smyčka	Libanon loop	Technické zařízení podvodně umístěné do čtečky karty v bankomatu s cílem neoprávněného získání platební karty.
Logo	Brand mark	Výlučná kombinace jména, symbolů a barev, která vizuálně vyjadřuje identitu značky (ochranné známky).
Maestro	Maestro	Ochranná známka a servisní značka používaná pro globální on-line debetní produkt asociace MasterCard. Tento produkt má povinné

		používání PIN při transakcích v místě prodeje a u transakcích v bankomatech.
Magnetický proužek	Magnetic stripe	Součást platební karty sloužící k záznamu elektronických údajů.
Majitel účtu	Account owner	Majitel účtu je fyzická nebo právnická osoba, na jejíž jméno je účet veden. Právnická osoba jedná prostřednictvím statutárního zástupce.
Manuální transakce	Manual transaction	Transakce, pro niž obchodník získal detaily karty manuálně. Detaily karty je možné získat otiskem (imprintem) karty v prodejním místě nebo je uvést v korespondenci nebo telefonickém příkazu (nikoli však elektronicky prostřednictví terminálu v prodejním místě). Viz též Manuální otisk.
Mechanický imprinter	Imprinter	Mechanické zařízení sloužící k pořízení otisku údajů z embosované platební karty na prodejní doklad.
Metoda autentikace karty	Card Authentication Method	Proces, kterým je platební karta ověřena jako právoplatná, nikoli padělaná. Pozn. U karty s magnetickým proužkem zahrnuje např. kontrolu hologramu, který může být zkontrolován obchodníkem, resp. zašifrovaných dat na magnetickém proužku, která může zkontrolovat vydavatel karty. V anglické zkratce CAM.
Metoda ověření držitele karty	Cardholder Verification Method	Metoda, která ověřuje identitu držitele karty. Právoplatnost držitele karty může být ověřena například prostřednictvím podpisu, PINu nebo biometrických údajů. Ve zkratce CVM.
Mondex	Mondex	Název značky platební aplikace s čipovou technologií k uložení předem autorizované peněžní částky na platební kartě. Viz též Elektronická peněženka / Electronic purse.
Multiple imprint	Multiple imprint	Podvodné vícenásobné vyhotovení prodejního dokladu bez vědomí držitele karty.
Neoprávněná transakce	Unauthorised transaction	Transakce provedená bez vědomí právoplatného držitele karty.
Obchodní místo	Merchant outlet	Též obchodní provozovna nebo prodejní jednotka, přijímající platební kartu k úhradě zboží nebo služeb, a to s obsluhou nebo samoobslužně (např. prostřednictvím samoobslužného terminálu, bankomatu nebo internetového serveru). Pozn. Obchodní místo označuje buď: - fyzické prostory, kde je provedena transakce platební kartou, v případě elektronického obchodování nebo Mail/Phone Order Merchant se jedná o stát, na který se vztahují všechny následující podmínky: - existuje trvalé sídlo obchodní společnosti, obchodníka (Permanent Establishment), jehož prostřednictvím se transakce provádějí - Obchodní společnost je držitelem platné licence pro obchodní místo - Obchodní společnost udržuje místní adresu pro korespondenci a právní jednání - Obchodní místo platí daně ve vztahu ke své prodejní činnosti.Viz též Obchodní společnost / Merchant, Prodejní místo / Point-of-sale, Místo transakce / Point-of-transaction.
Odmítnutí	Decline	Typ autorizační odpovědi, který používá vydavatel (nebo jeho agent nebo jedna ze služeb Stand-in / On-behalf) k odmítnutí autorizace transakce.
Off-line ověření	Off-line PIN	Proces používaný k ověření identity držitele karty porovnáním typovaného

PINu	Verification	PINu do čtečky PINu s hodnotou PINu uloženou v čipu.
Ochranná známka	Brand	Identita konkrétního platebního produktu, k jehož používání na daném území byla udělena licence. Ochranné známky kartových asociací zahrnují např.: MasterCard, Maestro, Cirrus, Euro Traveller Cheque (Cestovní šek euro), VISA, VISA Electron, MC Securicode, Verified by Visa, PayByTouch.
Oprávněný držitel karty	Cardholder	Fyzická osoba, pro kterou byla vydavatelem vydána platební karta.
OTP	One Time Password	Jednorázový autentikační kód.
Ověření čísla karty	Account number verification	Postup při kterém člen asociace nebo jeho autorizovaný zpracovatel zjišťuje pro trasankce, u kterých není vyžadována autorizace, zda v Exception File nejsou k číslu karty vedeny negativní informace.
Ověření PINu	PIN Verification	Bezpečnostní postup při ověření identity držitele karty, který umožňuje vydavateli karty zjistit, zda při žádosti o autorizaci držitel karty zadal na prodejním místě správný PIN.
Ověření podpisu	Signature verification	Bezpečnostní postup používaný pracovníkem prodejního místa ke zjištění oprávněnosti držitele karty k provedení transakce porovnáním podpisu držitele karty na vytištěném platebním dokladu transakce s podpisem na podpisovém proužku na kartě.
Padělaná karta	Counterfeit card	Karta, která byla vyrobena a personalizována bez souhlasu vydavatele nebo taková, která byla právoplatně vydána, ale později byla vizuálně upravena nebo byla pozměněna její elektronická data.
Phishing	Phishing	Snaha vylákat osobní nebo důvěrné informace například prostřednictvím náhodně rozesílaných e-mailů, které předstírají, že jejich autorem je důvěryhodná společnost. Jejich smyslem je přimět adresáta ke sdělení osobních nebo důvěrných informací, které mohou být následně zneužity. Vzniklo úpravou anglického výrazu fishing (rybaření) - vyslovuje se "fišing"; v češtině též jako "rhybaření".
Pick-up	Pick-up	Odpověď vydavatele na autorizační dotaz (obvykle jako kód autorizační odpovědi), ve které vydavatel požaduje od acquirera, aby karta účastná transakce byla terminálem nebo obchodníkem fyzicky stažena z oběhu, pokud je to bezpečně možné. Transakce sama je odmítnuta a musí být zrušena.
PIN - Osobní identifikační číslo	PIN - Personal Identification Number	Alfanumerický kód určený k autentikaci oprávněného držitele karty. Vydavatel jej sděluje výhradně oprávněnému držiteli karty, který má povinnost udržovat PIN v tajnosti.
PIN klávesnice	PIN pad	Klávesnice typu tamper-resistant určená pro bezpečné typování PINu a jeho zašifrování. Vyhovuje požadavkům ISO 9564-1.
Platební aplikace	Payment application	Softwarová aplikace uložená v čipu, která definuje parametry zpacování kartových transakcí odpovídající asociace.
Platební karta	Payment card	Nástroj sloužící k bezhotovostní úhradě zboží a služeb nebo výběru hotovosti. Ve smyslu zákona č. 124/2002 Sb. je považována za elektronický platební prostředek.

Platební nástroj	Payment instrument	Jakákoli karta, šek nebo jiný prostředek používaný k platbě za zboží nebo služby nebo k získání hotovosti.
Platební systém	Payment system	Odvětvový termín pro systém, který umožňuje převod peněz.
Platební terminál	Terminal	Technické zařízení umístěné na obchodním místě, určené k autorizaci platební transakce a jejímu vypořádání.
Platnost karty	Expiration date, expiry date	Údaj na platební kartě vymezující období, kdy lze kartu použít. Na přední straně platební karty je uveden ve tvaru MM/RR a zároveň je uložen v elektronické podobě na magnetickém proužku nebo čipu.
Podezřelá transakce	Suspisious transaction	Transakce, u které existuje pochybnost, zda byla provedena oprávněným držitelem karty, nebo o které držitel karty prohlásil, že ji neuskutečnil.
Podpisový proužek	Signature panel	Součást platební karty, kde je umístěn podpis držitele karty (vlastnoruční podpis nebo podpis provedený jinou technologií, např. laserem nebo přenesený fotograficky). Porovnáním podpisu na platební kartě s podpisem na prodejním dokladu je provedena autentikace.
Podvod bez přítomnosti karty	Card not present fraud	Podvod, při kterém buď platební karta nebo držitel karty nejsou fyzicky přítomni na místě uskutečňovaného prodeje. Podvodníci využívají podvodně získaná data o platební kartě k provedení nákupu prostřednictvím písemné, telefonické, faxové nebo internetové objednávky.
Podvod kartou ztracenou v poště	Mail non-receipt fraud	Podvod je založen na zcizení karty během přepravy od vydavatele karty před tím, než ji mohl převzít právoplatný držitel karty, a jejím následném zneužití neoprávněným držitelem.
Podvod padělanou kartou	Counterfeit card fraud	Podvod je založen na použití padělané karty, která byla vyrobena a personalizována bez souhlasu vydavatele nebo taková, která byla právoplatně vydána, ale později byla vizuálně upravena nebo byla pozměněna její elektronická data. Viz též Skimming.
Podvod se zcizenou identitou	Identity theft fraud	K podvodu se zcizenou identitou dochází použitím podvodně získaných osobních údajů. K využití zcizené identity může dojít dvěma způsoby: prostřednictvím podvodné žádosti o kartu nebo převzetím účtu.
Podvod ztracenou nebo zcizenou kartou	Lost and stolen card fraud	Podvody ztracenou nebo zcizenou kartou jsou podvody provedené takovouto kartou. Ztracená nebo zcizená platební karta je originální platební karta, která se dostane mimo fyzickou kontrolu oprávněného držitele karty.
POS	POS	Zkratka Point of Sale, Point of Service (prodejní místo, místo prodeje, místo obsluhy). Viz Prodejní místo / Point of Sale resp. Místo transakce / Point of Transaction.
Prodejní doklad	Sales draft, sales voucher, sales slip	Doklad o bezhotovostní platbě provedené platební kartou autentikované podpisem držitele karty nebo jeho PINem.
Prostředí bez přítomnosti karty	Card-Absent Environment	Prostředí, ve kterém je transakce provedena za obou uvedených podmínek:držitel karty není přítomen- karta není přítomna.Transakce v uvedeném prostředí zahrnují: transakce elektronického obchodování, písemné/telefonické objednávky, opakující se transakce, transakce telefonních služeb.
Předplacená	Prepaid Card	Karta používaná k přístupu na předplacený účet nebo karta, jejíž peněžní

karta		hodnota je uložena na čipu.
Referenční číslo zpracovatele	Acquirer´s reference number	Jedinečné číslo přidělené transakci zpracovatelem a používané k identifikaci původní finanční transakce během zúčtování (délka 23 číslic). Stejné číslo se používá během celého životního cyklu transakce. Ve zkratce ARN.
Scam mail	Scam mail	Scam = podfuk, bouda. Nevyžádaná elektronická pošta, kterou se odesílatel snaží získat důvěrné informace od příjemce. V některých státech je postavena na úroveň trestného činu.
Skimming	Skimming	Postup, při kterém jsou originální údaje z magnetického proužku karty elektronicky zkopírovány na jinou kartu bez vědomí právoplatného držitele karty.
Skimmovací zařízení	Skimming device	Technické zařízení umožňující zkopírování elektronických údajů z platební karty.
Stop list	Stop list	Soubor dat v papírové nebo elektronické formě obsahující čísla blokovaných karet, které nesmějí být akceptovány k provedení transakce. Využití stop listu při autorizaci zabraňuje zneužití zablokované karty.
Stopa	Track	Definovaná část magnetického záznamového média, kam lze zapisovat data. U platebních a bankovních karet magnetický proužek na rubu karty je rozdělen do tří podélných stop, z nichž každá může obsahovat zašifrovaná data v definovaném formátu.
Terminál	Terminal	Zařízení, které umožňuje uživateli posílat data do vzdáleného počítačového systému, přijímat z něj data nebo nové funkce (tzv. download). U kartových transakcí se terminál používá k předání dat o kartě vydavateli a realizaci transakce nákupu zboží a/nebo služeb. Viz též Terminál v místě prodeje / POS terminal.
Terminál off-line	Off-line terminal	Terminál obchodníka, který u každé transakce shromažďuje a ukládá data o kartě a transakci. Údaje za všechny transakce uložené v paměti terminálu jsou pravidelně (zpravidla na konci každého dne) posílána acquirerovi.
Terminál on-line	On-line terminal	Terminál obchodníka, který u každé transakce shromáždí údaje o kartě a transakci a odesílá žádost o autorizaci transakce.
Terminál samoobslužný	Cardholder Activated Terminal	Terminál aktivovaný držitelem karty, který vydává produkt nebo poskytuje službu (např. prodej pohonných hmot, nápojů, úhrada parkovného, mýta apod.). Viz též Transakce aktivovaná držitelem karty. Ve zkratce CAT.
Transakce	Transaction	Bezhotovostní platba prostřednictvím platební karty za zboží nebo služby anebo výběr hotovosti kartou. Probíhá v několika fázích: zahájení s ověřením držitele, schválení (autorizace) platby, vyhotovení dokladu a zúčtování.
Transakce aktivovaná držitelem karty typu A	Cardholder-Activated Transaction Type A	Transakce, která byla aktivována u samoobslužného terminálu a má všechny následující charakteristiky: - je na nižší částku než 40 USD nebo ekvivalent v místní měně - není autorizována - nebylo provedeno ověření držitele karty. Příklady Transakce typu A: poplatek za stání v halových garážích, dálniční mýtné, vstupné do kin, telefonní hovory.

Transakce aktivovaná držitelem karty typu B	Cardholder-Activated Transaction Type B	Transakce, která byla aktivována u samoobslužného terminálu a má všechny následující charakteristiky: - je na nižší částku než 100 USD nebo ekvivalent v místní měně- je autorizována- nebylo provedeno ověření držitele karty. Příklady Transakce typu B: nákup pohonných hmot bez použití PIN, nákup předplacené karty, vypůjčení videa.
Transakce aktivovaná držitelem karty typu C	Cardholder-Activated Transaction Type C	Transakce, která byla aktivována u samoobslužného terminálu a má obě následující charakteristiky: - je autorizována - bylo provedeno ověření PINu. Příklady Transakce typu C: nákup pohonných hmot s použitím PIN.
Transakce dobití	Load Transaction	Transakce k doplnění peněžní hodnoty do čipové karty prostřednictvím bankomatu nebo zvláštního zařízení (Load Device).
Transakce MO/TO	MO/TO transaction	Viz Transakce na podkladě písemného/telefonického příkazu / Mail order/telephone order transaction.
Transakce na podkladě písemného/telefonického příkazu	Mail order/telephone order (MO/TO) transaction	Transakce iniciovaná držitelem karty prostřednictvím buď korespondence s obchodníkem nebo instrukcí daných obchodníkovi telefonem, přičemž ani karta ani držitel karty není na prodejním místě přítomen.
Transakce ověřená PINem	PIN based transaction (PBT)	Transakce, u které je autentikace držitele karty provedena ověřením PINu zadaného držitelem karty v prodejním místě.
Transakce ověřená podpisem	Signature based transaction (SBT)	Transakce, u které je autentikace držitele karty provedena ověřením podpisu držitele karty v interakčním místě fyzickým porovnáním podpisu držitele karty s podpisem, který je uveden na podpisovém proužku karty.
Typování PIN	Typing PIN	Zadání PINu prostřednictvím PIN klávesnice. Jedná se o jeden ze způsobů autentikaci držitele karty.
Virtuální karta	Virtual card	Platební karta, existující pouze ve formě čísla karty, určená pro použití na internetu. Nemá fyzickou (plastovou) podobu, a proto nemůže být použita v prostředí "z očí do očí" (kde je pro realizaci transakce vyžadována fyzická přítomnost karty).
Virtuální účet	Virtual Account	Zákaznický účet, ke kterému nebyla fyzicky vydána karta; zakládá se pro realizaci transakcí při elektronickém obchodování.
Vydavatel karty	Issuer	Banka, úvěrová nebo jiná finanční instituce, která vydává platební karty a která má smluvní vztah s držitelem karty.
Zablokování karty	Card blocking	Akce, která znemožní další používání platební karty. Zablokovanou kartu již nelze používat k realizaci autorizovaných transakcí.
Znehodnocení karty	Card invalidation	Způsob narušení celistvosti platební karty zabraňující jejímu dalšímu použití. Provádí se v souladu s pokyny vydavatele karty. Pokud vydavatel znehodnocení nespecifikuje, kartu je třeba znehodnotit podélným rozstřižením v místě čísla karty a proděravěním magnetického proužku nebo čipu.

Příloha č. 2 – Bankomaty, platební karty

Obrázek 12 – Bankomat s nasazeným skimmovacím zařízením – falešný nástavec na vstupní štěrbinu pro platební kartu a falešný celý spodní panel s klávesnicí.

Obrázek 13 – Detail falešného nástavce s otvorem pro vsunutí platební karty (v pravé části otvoru je vidět snímač magnetického proužku karty.

Obrázek 14– Detailní pohled na zadní stranu nástavce na vstupní štěrbinu pro vsunutí platební karty se snímačem magnetického proužku karty, ovládací elektronikou a čipem na ukládání dat (pravá strana) a napájecí baterií.

Obrázek 15 – Detailní pohled na falešnou klávesnici ve falešné spodní desce nasazené na originální klávesnici.

Obrázek 16– Detailní pohled na zadní stranu falešné spodní desky s falešnou klávesnicí, propojenými tlačítky, ovládací elektronikou, akubaterií a čipem na záznam kódů PIN.

Obrázek 17– Ukázka upraveného pokladního terminálu zajištěného dánskou policií.

Obrázek 18 – Čtečka - zapisovačka karet

Obrázek 20– Čisté karty

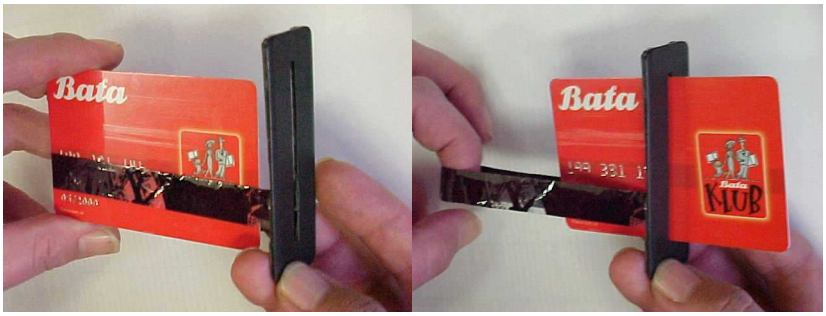
Obrázek 19– Odcizené platební karty

Obrázek 21– Bankomat se skimmovacím zařízením
Obrázek 22– Detail falešné spodní desky.

Obrázek 23– Celý falešný panel
Obrázek 24– Jiný typ falešného spodního panelu na bankomatu.

Obrázek 25– Přední část falešného nástavce jiný typ
Obrázek 26– Zadní strana falešného nástavce.

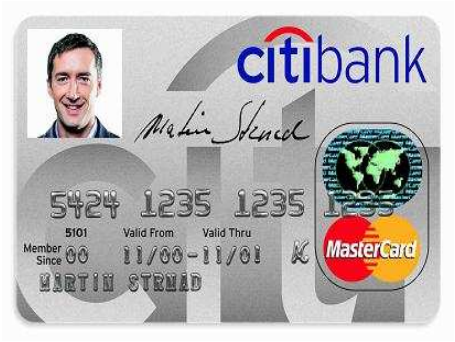
Obrázek 27– Tzv. „ libanonská smyčka“



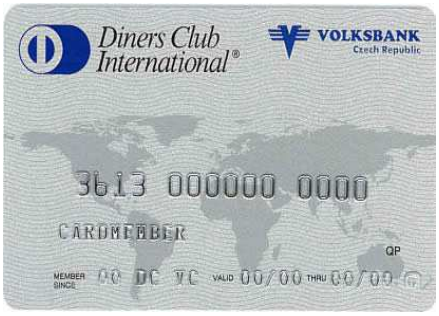
Obrázek 28 – Neoprávněný způsob vyjmutí platební karty

Obrázek 29 – Čtečka magnetického proužku

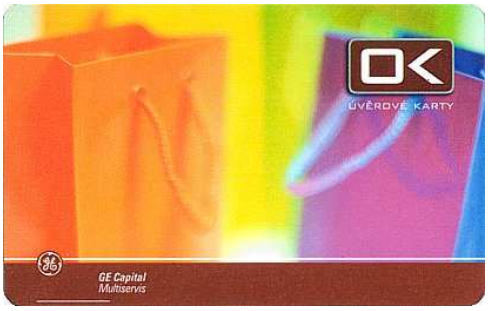
Obrázek 30 – Debetní karta (debit cards)



Obrázek 31 – Kreditní karta (credit cards)



Obrázek 32 – Charge karta (charge cards)



Obrázek 33 – Nákupní úvěrové karty

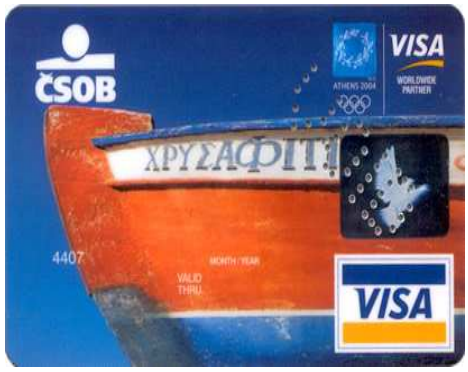
Obrázek 34 – Embosované karty

Obrázek 35 – Karty podle vydávajících asociací

Obrázek 36 – Karty VISA Silver,Gold, Platinium pro vyšší třídu klientů

Obrázek 37 – Karty Diners Club, JCB a AMEX – bonitnější klienti, exklusivní platební nástroj

Obrázek 38 – Karty podle použitelnosti klienti, exklusivní



Obrázek 39 – Karty mezinárodní klienti, exklusivní platební nástroj

Obrázek 40 – Hybridní karty

Obrázek 41 – Karty virtuální

Příloha č.3 – Stanovisko NSZ

Nejvyšší státní zastupitelství

SL 736/2007

Sbírka výkladových stanovisek
Nejvyššího státního zastupitelství
V Brně dne 22. srpna 2007

Poř. č. 2/2007

Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k možnosti postihu jednání osoby spočívajícího v padělání či pozměňování platební karty jako trestného činu padělání a pozměňování peněz podle § 140 odst. 2, § 143 trestního zákona

----

Úmyslné jednání pachatele spočívající ve zhotovení napodobeniny (kopie) bezhotovostního platebního prostředku v takové kvalitě, že mu to umožní realizovat neoprávněně bankovní operaci (obchod), lze posoudit jako trestný čin padělání a pozměňování peněz podle § 140 odst. 2, § 143 trestního zákona. Takto je možno kvalifikovat i jednání pachatele, který provede bankovní operaci prostřednictvím bankomatu použitím napodobeniny platební karty - plastikové karty opatřené překopírovaným magnetickým proužkem, případně údaji získanými z čipu.

Policejní prezidium Policie České republiky požádalo prostřednictvím odboru bezpečnostní politiky Ministerstva vnitra Nejvyšší státní zastupitelství o zaujetí stanoviska ohledně nejednotné aplikace ustanovení § 140, § 143, resp. § 249b tr. zák., pokud jde o právní posouzení trestního postihu výroby a padělků platebních karet. Dle jeho názoru, výklad této problematiky tak, jak jej obsahuje komentář k trestnímu zákonu autorů Šámal a kol., vydaný nakladatelstvím C.H. Beck, je nesprávný a prakticky je v rozporu se zásadou spravedlivého trestu. Jde o výklad, který považuje za padělek

platební karty jako bezhotovostního platebního prostředku pouze kartu, která má všechny náležitosti skutečné platební karty (např. označení vydavatele platební karty, jméno držitele, číslo a platnost platební karty, záznam dat, barevné provedení). Karta, která nemá všechny tyto náležitosti, je považována za pouhou napodobeninu karty, tzv. náhražku.[84] Akceptace tohoto právního názoru znamená, že jednání v souvislosti s *padělkem* platební karty je postihováno jako trestný čin padělání a pozměňování peněz podle ustanovení § 140 a § 143 tr. zák. s trestní sazbou minimálně dvě až osm let odnětí svobody, prakticky totožné jednání se stejným následkem v souvislosti s *napodobeninou (náhražkou)* jako trestný čin neoprávněné držení platební karty podle § 249b tr. zák., kde je trestní sazba minimálně dvě léta odnětí svobody.

Nejvyšší státní zastupitelství zjistilo dotazem u státních zastupitelstvích nižších stupňů, že jakkoli je frekvence tohoto druhu trestné činnosti v podstatě nízká, neexistuje zcela jednotný názor právě na problém právní kvalifikace jednání pachatele, který použije k realizaci bankovní operace prostřednictvím bankomatu plastikové karty neoprávněně opatřené magnetickým proužkem, která tuto operaci umožňuje. Většinově převládá názor, že jednání spočívající ve výrobě či užití takového padělku platební karty, či předmětu schopného plnit alespoň některou z jeho funkcí, naplňuje znaky trestného činu padělání a pozměňování peněz podle § 140 tr. zák., za použití § 143 tr. zák.

Část nižších státních zastupitelství považuje za padělek bankovní platební karty pouze takový předmět, který byl neoprávněně zhotoven s cílem, aby vykazoval charakteristiky vzhledu i obsahu pravé bankovní platební karty. Pokud takto vyrobený předmět nemá charakteristiku vzhledu a obsahu platební karty, lze jej považovat jen za náhražku s možným trestním postihem pouze jako trestný čin neoprávněného držení platební karty podle § 249b tr. zák. Vnější podoba upravených plastikových karet, kdy jsou bez jakéhokoli pokusu o napodobení platební karty, resp. napodobení jejích vnějších grafických znaků, pouze za pomoci technických prostředků překopírovány datové záznamy, je podle tohoto názoru zcela zjevně nezpůsobilá k jakékoliv záměně s pravými bankovními platebními kartami, a tedy nezpůsobilá vyvolat v představě příjemce omyl ohledně pravosti.

[84] Srov. P. Šámal - F. Púry - S. Rizman: Trestní zákon. Komentář. 6. přepracované vydání. C. H. Beck, Praha 2004, str. 885

Trestného činu padělání a pozměňování peněz podle § 140 odst. 2 tr. zák. se dopustí, kdo padělá nebo pozmění peníze v úmyslu udat je jako pravé nebo platné anebo jako peníze vyšší hodnoty, nebo kdo padělané nebo pozměněné peníze udá jako pravé.

Podle § 143 tr. zák. platí, že ochrana podle § 140 až § 142 tr. zák. se poskytuje též penězům cizozemským, tuzemským a cizozemským bezhotovostním platebním prostředkům, jakož i tuzemským a cizozemským cenným papírům.

Z publikovaných rozhodnutí Nejvyššího soudu, která se vztahují k tomuto druhu trestné činnosti, je relevantní především rozh. č. 21/2001 Sb. rozh. tr. konstatující, že *jestliže příkaz k úhradě jako bezhotovostní platební prostředek je padělán nebo pozměněn takovým způsobem, že obsahuje zdánlivě správné a reálné údaje, které jsou potřebné a způsobilé k uskutečnění platebního styku, pak v jednání pachatele, který jej takto padělá (pozmění) v úmyslu uskutečnit jeho prostřednictvím platební styk, popř. takový příkaz k provedení platebního styku předloží, lze spatřovat trestný čin padělání a pozměňování peněz podle § 140 odst. 2 tr. zák. za použití § 143 tr. zák.*

Bezhotovostním platebním stykem probíhajícím zpravidla prostřednictvím bank se uskutečňují převody peněz pomocí bezhotovostních platebních prostředků. Jedná se tedy o instrumenty sloužící k realizaci a usnadnění bezhotovostního platebního styku. Nutno především vyjít ze skutečnosti, že žádný obecně závazný právní předpis nestanoví ani taxativní výčet těchto instrumentů ani jejich obligatorní náležitosti. Za bezhotovostní platební prostředky je potřeba považovat jak ty, které jsou příkladmo uvedeny v zákoně č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, tak i instrumenty jiné sloužící k tomuto účelu v zákoně neuvedené. Nejvyšší státní zastupitelství řešilo tuto otázku v souvislosti s pochybnostmi, zda bezhotovostním platebním prostředkem je i příkaz k úhradě (inkasu) v zákoně o bankách neuvedený.[85]

Pokud se jedná o **bankovní platební karty**, žádný obecně závazný právní předpis České republiky neobsahuje jejich speciální právní úpravu ani vymezení jejich charakteru. Rámcové rozhodnutí Rady ze dne 28. května 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků jistým způsobem platební kartu definuje, když stanoví, že *pro účely tohoto rámcového rozhodnutí se rozumí „platebním nástrojem“ hmotný nástroj s výjimkou zákonného platidla (bankovek a mincí), díky němuž*

[85] Srov. výkl. stan. č. 15/2000 Sb. v. s. NSZ

*může držitel nebo uživatel na základě jeho specifické povahy samostatně nebo ve spojení s jiným (platebním) nástrojem převést peníze nebo peněžní hodnotu, jako jsou například kreditní karty, karty Eurocheque, jiné karty vydané finančními institucemi**, c**estovní šeky, eurošeky, jiné šeky a směnky, které jsou například provedením, kódováním nebo podpisem chráněny před napodobením nebo podvodným použitím.*[86]

Závaznými vnitrostátními právními předpisy je pouze upravena ochrana platebních karet před jejich padělám, pozměňováním a neoprávněnou držbou (trestní zákon, zákon č. 200/1990 Sb., o přestupcích, vyhláška České národní banky č. 36/1994 Sb., o podmínkách, za kterých lze reprodukovat bankovky, mince, šeky, cenné papíry a platební karty a vyrábět předměty, které je úpravou napodobují).

Podrobnější - nikoliv však obecně závaznou úpravu vztahů týkajících se platebních karet obsahují obchodní podmínky jednotlivých peněžních ústavů, podle kterých postupují při vydávání svých platebních karet. Tyto obsahují konkrétní náplň používání platební karty a jsou nedílnou součástí smlouvy o vydání a používání karty uzavřené mezi majitelem účtu a peněžním ústavem a v rámci tohoto vztahu se stávají závazné pro strany, které danou smlouvu uzavřely. Důsledkem porušení podmínek ze strany klienta může být vypovězení smlouvy a následné zablokování karty jejím vydavatelem. Obchodní podmínky jsou vystavěny na určitých zásadách, jimiž se řídí vydávání a používání platebních karet. Jejich znění bylo zakotveno v Úředním sdělení České národní banky č. 31/1994 Sb., o vydání Všeobecných obchodních podmínek (dále jen „VOP“), kterými se stanoví zásady vedení účtů klientů u bank a provádění platebního styku a zúčtování na těchto účtech, ve znění Úředních sdělení č. 18/ 1997 Sb. a č. 12/2000 Sb.

VOP v podstatě žádným způsobem nevymezuje právní statut platební karty ani neobsahuje ustanovení, které by jednoznačně zařadilo platební kartu mezi bezhotovostní platební prostředky. V čl. 47 charakterizuje platební kartu jako platební prostředek, kterým klienti provádějí bezhotovostní platby a výběry hotovostí prostřednictvím účtu, vedeného u banky. Dále podrobně stanoví, jaké náležitosti musí platební karta obsahovat. Čl. 6 uvádí, že **klient provádí bezhotovostní platby převodem peněžních prostředků z účtu na účet prostřednictvím** těchto platebních prostředků: jednorázového nebo trvalého příkazu k zúčtování; příkaz k zúčtování vyhotovuje plátce (majitel účtu nebo osoba

[86] Srov. Rámcové rozhodnutí Rady č. 2001/413

oprávněná disponovat s peněžními prostředky na účtu) formou příkazu k úhradě, nebo příjemce (osoba, která není majitelem účtu, ani osobou oprávněnou disponovat s peněžními prostředky na účtu) formou příkazu k inkasu v případech stanovených v čl. 7 bodu 2 a v čl. 9 bodu 2, šeku z účtování [čl. 31 bod 1, písm. a)] a **bankovní platební karty**. Jakkoliv tedy není bankovní platební karta podřazena jednoznačně ani pod hotovostní, ani pod bezhotovostní platební prostředky, je skutečností, že její použití je možné jak k realizaci hotovostní, tak k realizaci bezhotovostní operace, přičemž trend v posledních letech směřuje jednoznačně ve prospěch použitelnosti platební karty ve funkci bezhotovostního platebního prostředku na úkor využívání platebních karet pouze pro výběr hotovosti z bankomatu, což je považováno za hotovostní platební styk. Použitím bankovní karty v bankomatu lze zadat jakýkoliv jednorázový platební příkaz k úhradě (k zaplacení jakékoliv složenky), lze dobíjet mobilní telefony a poukázat peníze na bankovní účet jiného komitenta. Pokud je tedy bankovní karta použita k realizaci bezhotovostního platebního styku, je ji třeba nepochybně považovat za bezhotovostní platební prostředek.

Kromě nesporných kladů usnadňujících a urychlujících platební styk s bankou má však masové používání platebních karet i svou negativní stránku spojenou s dost širokým spektrem možností jejich zneužití. K zamezení, přesněji řečeno, ke ztížení zneužití platebních karet, používají jejich emitenti různých způsobů ochrany, které se vztahují jednak k jejich vnějším vzhledovým znakům, které však nemusí být na první pohled viditelné a lze je např. ověřit pouze za pomocí specifických prostředků např. ultrafialové světlo), jednak k ochraně zakódovaných elektronických údajů. Aktivity padělatelů jsou namířeny proti oběma skupinám prostředků ochrany. Elektronická ochrana je realizována zakódováním údajů potřebných k použití karty především na magnetickém proužku, v posledním období se začíná uplatňovat ochrana údajů jejich zakódováním v čipu. V intencích právního problému, který řeší toto výkladové stanovisko, je důležité si uvědomit, že ne při každém použití platební karty je možno, před nebo v průběhu probíhající platební operace, provést kontrolu všech ochranných prvků, kterými je bezhotovostní platební prostředek vybaven. Jestliže při použití platební karty k přímé platbě zboží je možné provedení kontroly všech vnějších vzhledových znaků, při realizaci bankovní operace prostřednictvím bankomatu to možné není.

Pokud jde o úvahy vztahující se k požadavkům na úplnost a technickou kvalitu výslednosti aktivity padělatelů, tedy technickou kvalitu a vzhled napodobeniny z hlediska

její použitelnosti k provedení bankovní operace, Nejvyšší státní zastupitelství především zastává právní názor svědčící o nutnosti jednotného posuzování všech bezhotovostních platebních prostředků, tedy včetně platební karty, pokud je jako bezhotovostní platební prostředek používána, což však neznamená, že by všechny tyto prostředky musely být nutně padělány stejným způsobem. Rozhodující pro řešení daného problému je posouzení charakteru operace, kdy je prostřednictvím platební karty prováděn bezhotovostní platební styk nebo inkaso finanční hotovosti z bankomatu a případně odlišení této operace od případů, kdy je platební operace provedena pomocí jiných instrumentů - bezhotovostních platebních prostředků. Vzhledem ke skutečnosti, že používání bankomatu k realizaci bezhotovostních platebních operací a výběru hotovosti pomocí bankou vydané platební karty je součástí smlouvy o úvěru nebo vkladu, nemůže být žádných pochyb, že v obou případech jde o bankovní obchod. Vložení napodobeniny platební karty do bankomatu představuje tedy nepochybně způsob realizace obchodního styku s bankou. V podstatě jde o stejný případ, jako když je bance předložen jakýkoliv jiný bezhotovostní platební prostředek s požadavkem na provedení bankovní operace. Není rozhodné, zda je tato operace prováděna prostřednictvím bankovního úředníka nebo prostřednictvím bankomatu.

V případě akceptování správnosti tohoto názoru by bylo poté obtížné ztotožnit se s výkladem, jak vyplývá z citované části aktuálního komentáře k trestnímu zákonu, jehož dopad by v praxi mohl znamenat, že jednání pachatele, kdy pracovníku banky na přepážce předloží částečně padělaný příkaz k úhradě, který je pracovníkem banky akceptován a uvedená částka je pachateli vyplacena, přičemž jednání jiného pachatele, který pomocí částečně padělané platební karty – plastikové karty opatřené neoprávněně překopírovaným magnetickým proužkem či vybavené údaji získanými neoprávněně z čipu karty, realizuje prostřednictvím bankomatu neoprávněně bankovní obchod se stejným následkem, by bylo třeba z hlediska trestní odpovědnosti posuzovat podle rozdílných ustanovení trestního zákona.

Klíčovým momentem pro posouzení skutečnosti, zda napodobeninu bezhotovostního platebního prostředku je možno považovat za padělek ve smyslu ustanovení § 140 odst. 1 tr. zák. (ve spojení s § 143 tr. zák.) by mělo být zásadně zjištění, zda je napodobenina použitelná pro bankovní operaci (obchod), ke které je určena, přičemž postačí, v případě vícefunkční použitelnosti tohoto platebního prostředku, zjištění reálné možnosti provedení jedné operace. Jestliže tedy pro teoreticky úspěšné použití padělané směnky či

příkazu k úhradě, který je předkládán bankovnímu úředníkovi, je bezpochyby potřebné padělání i vnějších charakteristických prvků takových napodobenin, pro úspěšné použití napodobeniny platební karty k realizaci bezhotovostního platebního styku prostřednictvím bankomatu nebo výběru hotovosti z bankomatu je padělání takových odlišovacích prvků zjevně nepotřebné. Nelze se proto ztotožnit s názorem, že plastiková karta s překopírovaným magnetickým proužkem, případně vybavená údaji získanými neoprávněně z čipu karty, je zcela zjevně nezpůsobilá k jakékoliv záměně s pravými bankovními platebními kartami, a tedy nezpůsobilá vyvolat v představě příjemce omyl ohledně pravosti. Pokud takto upravenou napodobeninu bankomat akceptoval a požadovanou operaci provedl či vydal požadovanou finanční hotovost, bankovní operace (obchod) byla uskutečněna, nepochybně poté, kdy banka byla uvedena v omyl a kdy tedy nelze hovořit o nezpůsobilosti padělku k jakékoliv záměně s pravými bankovními platebními kartami. Akceptování stanoviska citovaného komentáře má tak za následek neadekvátní vymezení trestní odpovědnosti pachatelů včetně následného trestního postihu, který neodpovídá zjištěným skutečnostem v konkrétní trestní věci, což je možno považovat za porušení principu proporcionality trestně právní represe.

Existence skutkové podstaty neoprávněného držení platební karty podle ustanovení § 249b tr. zák. nemůže mít na platnost tohoto závěru žádný vliv. Z tohoto pohledu se spíše vnucuje otázka, proč z celé řady bezhotovostních platebních prostředků byla jednomu z nich tímto způsobem poskytnuta zvláštní ochrana.

Z hlediska výše uvedených úvah zastává Nejvyšší státní zastupitelství názor, svědčící pro plnou použitelnost rozh. č. 21/2001 Sb. rozh. tr. i na případy použití plastikové folie opatřené překopírovaným magnetickým proužkem, případně čipem, k výběru hotovosti z bankomatu. Je totiž možno konstatovat, stejně jako v odůvodnění tohoto rozhodnutí týkajícího se převodního příkazu, že byla předložena napodobenina bezhotovostního platebního prostředku plně způsobilá k úspěšné realizaci bankovní operace (obchodu).

Při posuzování, zda jde o padělek bezhotovostního platebního prostředku ve smyslu ustanovení § 140 tr. zák., by tedy mělo sehrát rozhodující roli zjišťování reálného předpokladu použitelnosti tohoto padělku (napodobeniny) pro uskutečnění bankovní operace (obchodu). Pokud toto zjištění vyústí do konstatování, že došlo k úmyslné neoprávněné výrobě napodobeniny jakéhokoli bezhotovostního platebního prostředku takovým způsobem a v takové kvalitě, které umožní pachateli

realizovat neoprávněně jakoukoliv bankovní operaci (obchod), jedná se vždy o padělání. Proto je třeba považovat za padělání i použití plastikové folie s překopírovaným magnetickým proužkem z platební karty, případně vybavené údaji získanými neoprávněně z čipu karty, pokud lze jejím použitím realizovat neoprávněně bankovní operaci (obchod). Pokud takovým jednáním pachatele došlo k realizaci výběru hotovosti z bankomatu, může být tento skutek, spáchaný v souběhu podřazen ještě pod jiné ustanovení trestního zákona.

Toto stanovisko bylo vydáno podle ustanovení § 12 odst. 2 zákona o státním zastupitelství.

Nejvyšší státní zástupkyně:
JUDr. Renata Vesecká, v.r.

Příloha č.4 - Poznámky:

[1] Mooreův zákon (1965, Gordon Moore – Intel) stanoví, že každých 18 měsíců dojde k zdvojnásobení výkonu mikroprocesoru za stejnou cenu nebo ekvivalentně pokles ceny na polovinu při nezměněném výkonu. K podobnému efektu dochází u kapacity komunikačních spojů, která se rovněž zvyšuje exponenciálně s poločasem zhruba 8 měsíců. Intel dodává, že zákon vydrží nejvýše do roku 2021 (zdroj: www.zive.cz).

[2] Podle manuálu OSN „United Nations Manual on Prevention and Control of Computer-Related Crime“ sem řadíme podvod, padělání, sabotáž počítačů, neoprávněný přístup k počítačovým programům a jejich neoprávněné kopírování.

[3] Massachusetts Institute of Technology.

[4] Nadace pro svobodný software založená roku 1985, jejím cílem bylo vytvořit systém podobný Unixu, tzv. GNU - nadace se stará o právní a organizační stránky projektu GNU a o rozšiřování povědomí o svobodném software.

[5] Bulletin Board System.

[6] Kevin Mitnick se stal nejstíhanějším hackerem všech dob, proslul také obratným využíváním sociálního inženýrství.

[7] Peer-to-peer – architektura sítě, ve které spolu komunikují přímo jednotliví uživatelé. P2P sítě slouží ke sdílení a anonymní výměně souborů po internetu.

[8] Zakladatelé Michael Karpor a John Barlow.

[9] Business Software Aliance.

[10] Principem hry je přerozdělování vložených finančních prostředků, částečně ve prospěch hráčů, částečně ve prospěch pořadatele podle daných priorit.

[11] Stav k 3. únoru 2005, zdroj: http://www.czech-talkpro.cz/-hps=stats.evropa.htm.

[12] Souhrnné označení veškerých nežádoucích programů - viry, červi apod.

[13] Program, který monitoruje úkony prováděné na počítači (zadávání hesel, spouštěné programy, psané e-maily apod.).

[14] Denial of Service, česky odepření služby - na rozdíl od počítačového viru nejde o infekci počítače, ale o jeho zahlcení či případné vyřazení z provozu.

[15] Slovní základ hack lze přeložit mnoha způsoby - rozsekat, rozřezat, otesávat, opracovávat, zaseknout, udělat zářez.

[16] Slovní základ crack znamená rozbít, rozlousknout.

[17] Speciální programy pro anonymní přijímání a odesílání zpráv (remailery) či prohlížení webových stránek. Remailery tak mohou být zneužívány pro šíření pornografie, extremismu, porušování AP.

[18] Network News Transfer Protokol – protokol pro přenos síťových zpráv.

[19] TCP (Transmission Control Protocol) – složitější nadstavbou nad protokolem IP a mění jeho způsob fungování – na spojitý a spolehlivý. Protokol TCP je spojovanou službou (connection oriented), tj. službou, která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh.

[20] Jednoznačný identifikátor počítače v síti internet.

[21] Virtuální privátní síť.

[22] Zdroj: http://www.ucdc.edu/aboutus/livingindc.cfm?dir=Faculty&id=15.

[23] Původ slova z malicious software.

[24] Původ slova z phone a freaks (podivíni).

[25] Původ slova z phone a crackers.

[26] Původ slova z password a fishing.

[27] Původ slova z password a farming.

[28] Manipulace, ovlivňování a klamání toho druhého, kdy je cílem od něj získat informace, které potřebujete, nebo ho přemluvit a zmanipulovat k tomu, aby třeba konkrétně do počítače zadal kód, který chcete, aby tam zadal.

[29] Zdroj: http://fpc.state.gov/documents/organization/45184.pdf.

[30] Používá se též zkratka UBE/UCE (Unsolicited Bulk/Commercial E-mail). Pro opak spamu, tj. žádanou poštu zaslanou konkrétní osobou se specifickým jednorázovým účelem, se řidčeji používá termín *ham* (zdroj: http://cs.wkipedia.org).

[31] Commtouch® Software Ltd. byla založena roku 1991 a specializuje na problémy e-mailové komunikace. Vyvíjí speciální detekční antispamový SW, poskytuje antivirovou ochranu uživatelům na celém světě. Monitoruje spamové aktivity, vytváří statistiky, nabízí kalkulátor nákladů, které firmy vynaloží na spam - samozřejmě s porovnáním nákladů vynaložených na nabízené antispamové řešení.

[32] Zdroj: http://www.getsafeonline.org.

[33] Pretty Good Privacy, tzn. „dost dobré soukromí“ (Phil Zimmerman, 1991). PGP je určeno pro bezpečný přenos elektronické pošty.

[34] BSA zohledňuje pouze případy týkající se přidružených výrobců SW.

[35] International Data Corporation (http://www.idc.com) – přední světová společnost v oblasti průzkumu trhu a poradenství pro ICT.

[36] Department of Justice – Ministerstvo spravedlnosti.

[37] Department of Justice – Ministerstvo spravedlnosti.

[38] Zentrale anlassunabhängige Recherche in Datennetzen.

[39] Zahrnujeme sem tzv. „zero-day“ útoky, které jsou zaměřeny na chyby výrobců SW a HW, dříve než stačí distribuovat opravné nástroje. Dále tzv. XENO (eXtended Enterprise Network Overseas), které se objevují v souvislosti s outsourcingem v oblasti IT. Poslední hrozbou v této oblasti jsou útoky na mobilní zařízení a bezdrátové produkty.

Příloha č.5 - Curriculum vitae

Jméno a příjemní:	Vladimír Šulc, Ing.
Datum a místo narození:	01.04.1964, Brno
Národnost:	ČR
Osobní stav:	ženatý
Adresa:	Jožky Jabůrkové 2, 624 00 Brno
Zaměstnavatel:	SPŠ MV v Brně, Horní 21, 659 65 Brno
Telefon, E-mail**:**	+420 605 714 895, Lada.Sulc@seznam.cz

Vzdělání:

1994 – 2001	Vysoké učení technické v Brně, Fakulta podnikatelská, obor daňové poradenství a podnikové finance a obchod
2004-dosud	studium v rámci doktorandského studijního programu na VUT v Brně, Fakultě podnikatelské.

Odborná praxe:

od roku 2000	odborný učitel v VPŠ MV V Brně.

Studijní pobyty:

březen-duben 2001	Chemnitz, SRN
červen 2004	Katowice, Polsko
září 2007	Bratislava, Chemnitz

Obor pedagogické činnosti:

- Semináře předmětu Hospodářská kriminalita
- Semináře předmětu Ekonomika a management
- Semináře předmětu Finance
- Semináře předmětu Finance podniku

Příloha č.6 – Další literatura

LITERATURA

1. BASL, J. *Podnikové informační systémy – Podnik v informační společnosti*. Praha: Grada, 2004. 144 s. ISBN 80-247-0214-2
2. BUCHALCEVOVÁ, A. *Metodiky vývoje a údržby informačních systémů*. Praha: Grada, 2004. 164 s. ISBN 80-247-1075-7
3. DOHNAL, J. *Řízení vztahů se zákazníky – Procesy, pracovníci, technologie*. Praha: Grada, 2004. 164 s. ISBN 80-247-0401-3
4. DONÁT, J. *E-Business pro manažery*. Praha: Grada Publishing, 2000. ISBN 80-247-9001-7
5. DOSTÁLEK, L. *Velký průvodce protokoly TCP/IP - Bezpečnost*. 2. vyd. Brno: Computer Press, 2003. 592 s.
6. DOUCEK, P. - BÉBR R. *Manažerské informační systémy a jejich ekonomika*. Praha: VŠE, 2002. ISBN80-245-0412-X
7. DVOŘÁK, J. - DVOŘÁK, J. *Elektronický obchod*. MSD s.r.o. Brno: Ing. Zdeněk Novotný, CSc, 2002. 116 s. ISBN 80-214-2236-X
8. FRIMMEL, M. *Elektronický obchod/právní úprava*. Praha: Prospektrum, 2002. ISBN 80-7175-114-6
9. HLAVENKA, J. *Dělejte byznys na internetu*. 2. vyd. Brno: Computer Press, 2004. 210 s.
10. CHLEBOVSKÝ, V. *CRM - Řízení vztahů se zákazníky*. Brno: Computer Press, 2005. 380 s.
11. CHEN, S. Strategic Management of e-Business. Hoboken, N. J.: John Willey, 2004. 366 s. ISBN 0-47-087073-7
12. JOHNSON, G. - SCHOLES, K. Cesty k úspěšnému podniku: stanovení cíle: techniky rozhodování. Praha: Computer Press, 2002. 803 s.ISBN 80-7226-220-3
13. KABELOVÁ, A. - DOSTÁLEK, L. Velký průvodce protokoly TCP/IP a systémem *DNS*. 3. vyd. Brno: Computer Press, 2003. 558 s.
14. KOISUR, D. *Elektronická komerce, principy a praxe*. Praha: Computer Press, 1998. 276s. ISBN 80-7226-097-9
15. KOPŘÍVA, P. *Elektronické podnikání*. [online] URL
16. KOSEK, J. *Přehled XML technologií a možností jejich využití*. [online] URL

17. LAMBET, D. - STOCK, J. - R., ELLRAM, L. *Logistika*. Brno: Computer Press, 2004. 612 s.
18. MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. 2. vyd. Praha: Grada, 2005. 180 s. ISBN 80-247-0087-5
19. NOVOTNÝ, O. - POUR, J. - SLÁNSKÝ, O. *Business Intelligence – Jak využít bohatství ve vašich datech*. Praha: Grada, 2005. 256 s. ISBN 80-247-1094-3
20. POSPÍŠIL, Robert. *EDI v kostce*. [online] URL
21. POUR, J. - GÁLA, L. - TOMAN, P. *Podniková informatika*. Praha: Grada, 2005. 256 s. ISBN 80-247-1278-4
22. POUR, Jan. *Informační systémy a elektronické podnikání*. Praha: VŠE, 2003. ISBN 80-245-0227-5
23. PLANT, R. *eCommerce: Formulation of Strategy*. Prentice Hall PTR, 2000. 368 s. ISBN 0-13-019844-7
24. RAFAJ, Nikola. *Nebezpečná bezpečnost*. [online] URL
25. SIXTA, J. - MAČÁT, V. *Logistika - teorie a praxe*. Brno: Computer Press, 2004. 320 s.
26. SMEJKAL, V. - BUDIŠ, P. - KODL, J. - MATES, P. *Elektronický podpis od A do Z*. Praha: Grada, 2005. 240 s. ISBN 80-247-0555-9
27. TONDR, L. Podnikáme s Internetem, 1. vyd. Praha: Computer Press, 2002. ISBN 80-7226-729-9
28. VRANA, I. - RICHTA, K. *Zásady a postupy zavádění podnikových informačních systémů – Praktická příručka pro podnikové manažery*. Praha: Grada, 2004. 188 s. ISBN 80-247-1103-6
29. VODÁČEK,L - VODÁČKOVÁ,O. *Malé a střední podniky: konkurence a aliance v Evropské unii*. Management Press. Praha 2004. ISBN 80-7261-099-6. s. 161
30. VOŘÍŠEK, J. Strategické řízení informačního systému a systémová integrace. 1.vyd. Praha: Management Press, 1999. 324s. ISBN 80-85943-40-9
31. RAIS, K. *Operační a systémová analýza.* Brno: skriptum VUT v Brně – Fakulta podnikatelská, 2001. 133 s. ISBN 80-214-1924-5
32. RODRYČOVÁ, D. - STAŠA, P. *Bezpečnost informací.* Vydala Grada Publishing, spol. s r.o.. 1.vydání. Praha 2000.144 stran.ISBN 80-7169-144-5.s. 93